Operations and Intelligence Report
METROBANK
March 2013

BEST IN CLASS – INFORMATION SECURITY
INTELLIGENCE AND OPERATIONS

1. About this report

The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the systems under contract. The information generated by these systems is then aggregated, correlated and analyzed. The more complete the set of systems under contract the more accurate and complete the results will be. The report is organized to provide an executive summary with recommendations (as necessary or applicable) followed by more detailed information.

We at GLESEC believe information security is a holistic and dynamic process. This process requires on-going research and follow up. Holistic since no single “device” can provide the security necessary for an organization. Technology alone cannot provide the security necessary, but people that understand the operations and information generated by the security devices are a key to proper security. The process is dynamic since due to the nature of Internet security given the constant discovery of new security vulnerabilities and exploits, the proliferation of hacking tools that make it easier for script-kiddies with minimal knowledge to cause damage. The increase in malware, phishing, insider threats, organized crime, and hacktivism are the very cause of information security exposure.

2. Confidentiality

GLESEC considers the confidentiality of client’s information as a trade-secret. The information in this context is classified as:

a) Client name and contact information
b) System architecture, configuration, access methods and access control
c) Security content

All the above information is kept secure to the extent in which GLESEC secures its own confidential information.

3. Executive Summary

This report corresponds to the period from MARCH 1, 2013 to MARCH 31, 2013

AppWall

Based on the information gathered from the AppWall during this period **16,007** attacks on METROBANK were all stopped by the Radware AppWall ODS1 XL.

The most prevalent vulnerability that was attacked during this report was Path Traversal. A Path Traversal attack aims to access files and directories that are stored outside the web root folder. By browsing the application, the attacker looks for absolute links to files stored on the web server. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations, it may be possible to access arbitrary files and directories stored on file system, including application source code, configuration and critical system files, limited by system operational access control. The attacker uses “../” sequences to move up to root directory, thus permitting navigation through the file system.

This attack can be executed with an external malicious code injected on the path, like the Resource Injection attack. To perform this attack it’s not necessary to use a specific tool; attackers typically use a spider/crawler to detect all URLs available. This attack is also known as “dot-dot-slash”, “directory traversal”, “directory climbing” and “backtracking”.

The second most common vulnerability that was attempted to exploit was Information Leakage. Information Leakage attacks attempt to reveal system data or debugging information helping an adversary learn about the system and form a plan of attack. An information leak occurs when system data or debugging information leaves the program through an output stream or logging function.

DefensePro

Based on the information gathered from the DefensePro during this period a total of **8,892** attacks on METROBANK, **161** of which were considered critical were stopped by the Radware DefensePro 506. During the previous period, **6,177** attacks on METROBANK, **274** of which were considered critical were stopped by the Radware DefensePro 506. Attack numbers increased overall for this report period, while critical attack numbers dropped.

The vast majority of attacks on METROBANK originated geographically from the following Top 10 countries: Panama, United States, China, Germany, United Kingdom, Venezuela, Japan, Italy, Canada, and Ireland listed in order of frequency. (Information and graph available in the Security Intelligence section of the report)

Approximately **71%** of the attacks registered on METROBANK are Packet Anomalies, specifically “TCP handshake violation, first packet not syn” packets. This anomalous traffic is usually caused by attacks or evasion tactics directed at the Network Access Control (NAC) devices such as firewalls in order to bypass their functions which if allowed to pass could permit scanning of the internal networks. They are also used as a method to collapse the underlying network infrastructures with packet crafting tools used by threat agents to interrupt services or distract security teams with volumetric attacks while more targeted attacks are directed at important assets to allow for data exfiltration. Packet Anomalies can also be caused by applications that do not adhere to RFC standards.

Scanning protection is much more effective this period due to the quarterly infrastructure review which was realized in conjunction with METROBANK staff and the GLESEC GOC. Scanning and reconnaissance accounted for **15%** of attacks during this report period. The threat agents were unsuccessful in utilizing blended multi-vector attacks in attempt to bypass protection mechanisms in order to enumerate the METROBANK infrastructure/services such as: TCP Scan, TCP Scan (horizontal), UDP Scan (vertical), TCP Scan (vertical). Network-wide Anti Scanning protections dropped enumeration attempts which otherwise thwart any effort for threat modeling, commonplace after the information gathering phase of a planned attack.

13 attacks on METROBANK are from known threat sources that have been compiled and correlated with attack source IPs gathered from the DefensePro and AppWall attack logs and outside sources such as honeypots, known malicious sources, relationships with CERT and CSIRT teams that GLESEC possesses, and various other threat feeds. (Information and graph available in the Security Intelligence section of the report)

Intrusion Rules and Server Cracking Protection assisted in preventing attacks directed at server level including the more common attacks suffered this period such as: Brute Force Web, Web Scan, SIP-Scanner-SIPVicious, HTTP Page Flood, Brute Force DNS, Brute Force SMB attacks which were directed at well-known port numbers: 443 (https), 80 (http), 445 (microsoft-ds), 5060 (sip), 8080 (http-alt), 53 (domain/dns), 25 (smtp) in order of frequency. Port number information utilized is based on IANA Service Name and Transport Protocol Port Number Registry.

4. Recommendations

GLESEC recommends “Implementing the First Five Quick Wins” based on the Twenty Critical Security Controls for Effective Cyber Defense, Version 4.1 that were formulated as a joint effort from the NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities. These are readily available from GLESEC which has provided the following link: https://www.sans.org/critical-security-controls/cag4-1.pdf

The Critical Controls represent the biggest bang for the buck to protect your organization against real security threats. Within Critical Controls 2-4 are five “quick wins.” These are subcontrols that have the most immediate impact on preventing the advanced targeted attacks that have penetrated existing controls and compromised critical systems at thousands of organizations.

The five quick wins are:

a) Application white listing (in CSC2)
b) Using common, secure configurations (in CSC3)
c) Patch application software within 48 hours (in CSC4)
d) Patch systems software within 48 hours (CSC4)
e) Reduce the number of users with administrative privileges (in CSC3 and CSC12)

METROBANK should consider adding SSL scrubbing/offloading to the protection strategy which allows for SSL sessions to be opened, analyzed, and dropped if considered malicious in nature due to the attacks on port 443 (https) which remain very high, which allow for encrypted attacks to enter the organization and affect the application layer without detection. METROBANK remains susceptible to these types of attacks.

5. Scope of this Report

The systems/services under this contract include:

Risk and Application	Countermeasures	GLESEC Services	Contracted
External layer security	Firewall	MSS-FW	No
External Layer Security	**Intrusion Prevention, DoS, NBA, Zero Day**	**MSS-APS**	**Yes**
Application Layer Security	**Application Firewall**	**MSS-APS**	**Yes**
Vulnerability Management	Vulnerability Management	MSS-VM	No
Internal Layered Security	End-Point Security	MSS-EPS	No
Centralized Alerting, Reporting and Intelligence	SIEM	MSS-SIEM	No
External and Internal Layer – Basic Infrastructure	DNS and IPAM	MSS-DNS	No
High Availability	Load Balancers – Links	SSP	No
High Availability	Load Balancers - Servers	SSP	No
Data Leakage Mobile Devices	Data Leakage Mobile Devices	SSP	No

GLESEC Services:
MSS: Managed Security Service (full outsourcing)
SSP: Security Support Program (systems management and support)

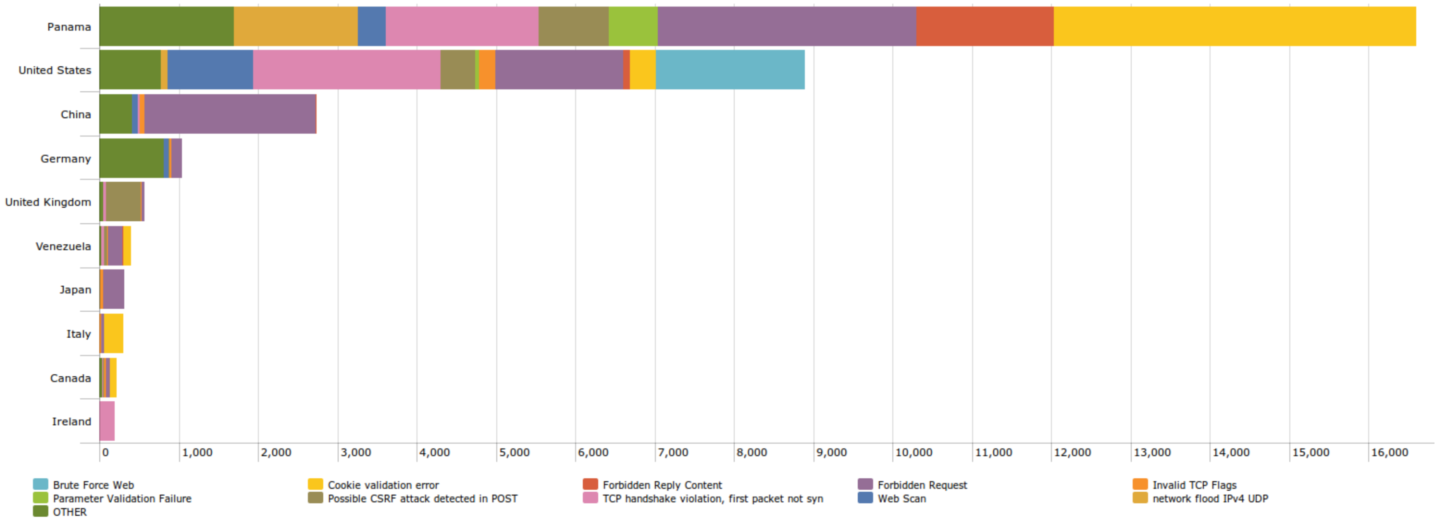
METROBANK Systems:
Radware DefensePro 506
Radware AppWall ODS1XL

6. Security Intelligence

The purpose of this section is to highlight intelligence gathered from the devices under contract as well as outside sources such as honeypots, known malicious sources, relationships with CERT and CSIRT teams that GLESEC possesses, and various other threat feeds.

The vast majority of attacks on METROBANK originated geographically from the following Top 10 countries: Panama, United States, China, Germany, United Kingdom, Venezuela, Japan, Italy, Canada, and Ireland listed in order of frequency.

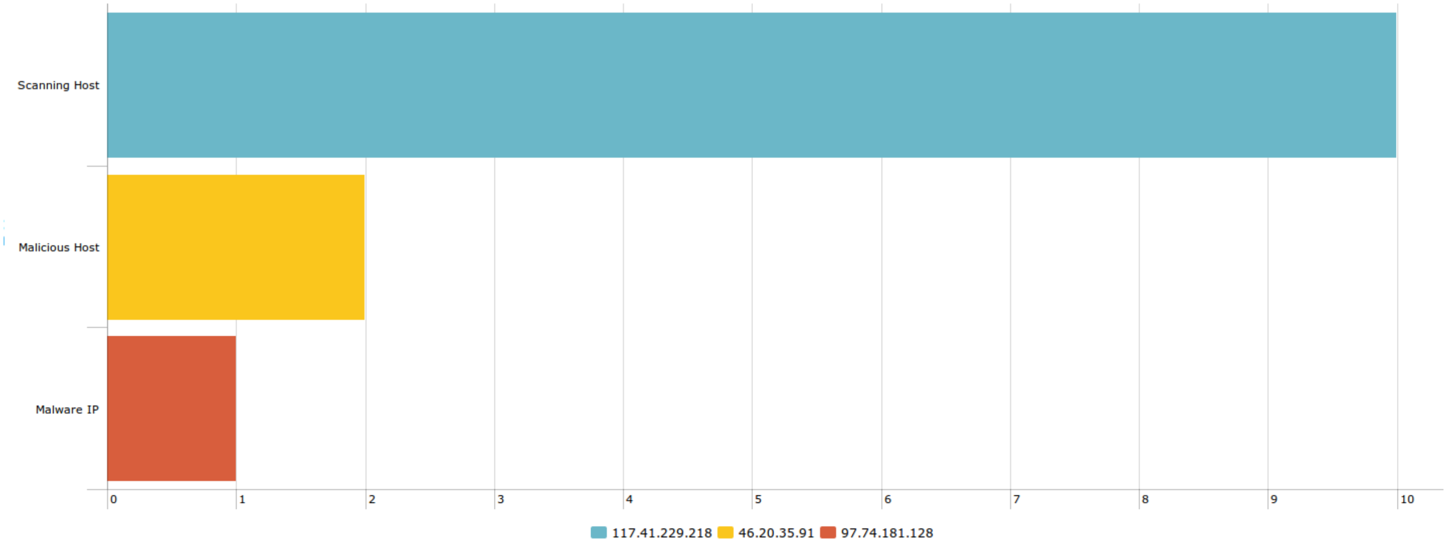
Graph: Top 10 Attacking Countries
This report provides the count of total attacks by country



13 attacks on METROBANK are from known threat sources that have been compiled and correlated with attack source IPs gathered from the DefensePro and AppWall attack logs and outside sources such as honeypots, known malicious sources, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

Graph: Known Threat Sources by Threat Type

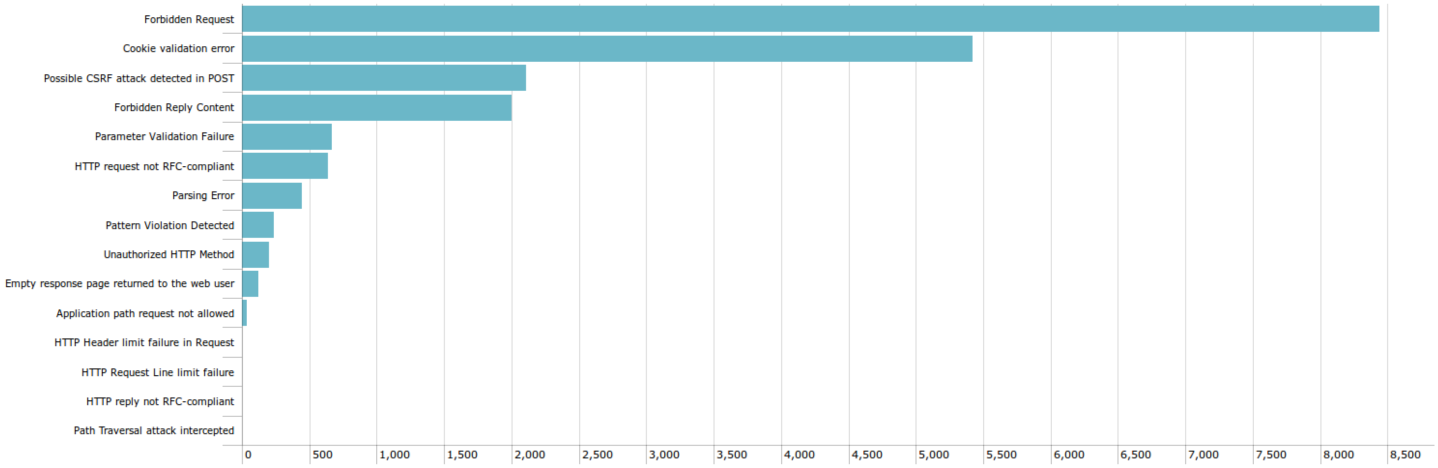
This report provides the count of known threat sources by IP and their respective infringing threat type. The category “OTHER” is a generic bucket for single IPs that have been grouped together.



AppWall

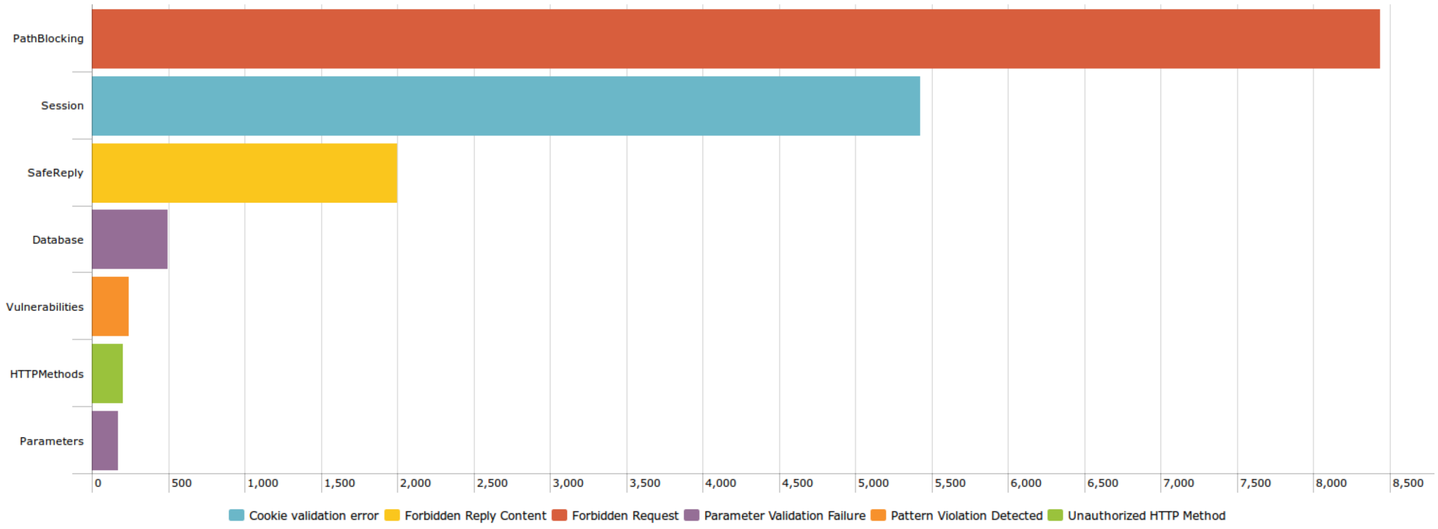
Graph: Top Attacks

This report provides the count of total attack types.



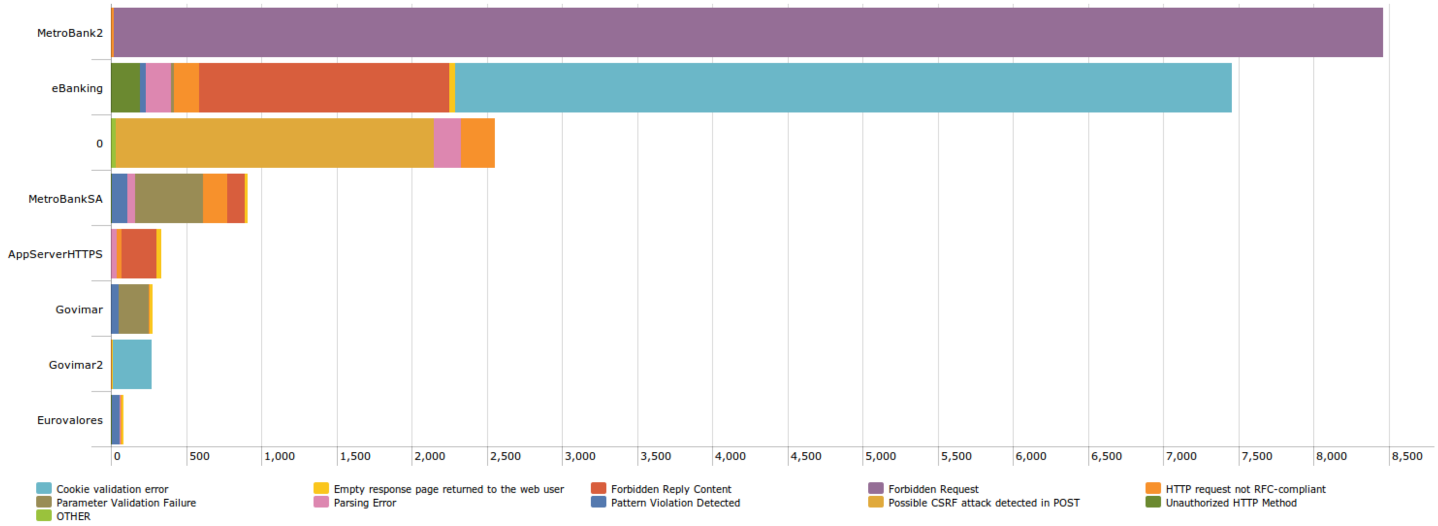
Graph: Top Objects by Attack

This report provides the count of attacks distributed over their related object..



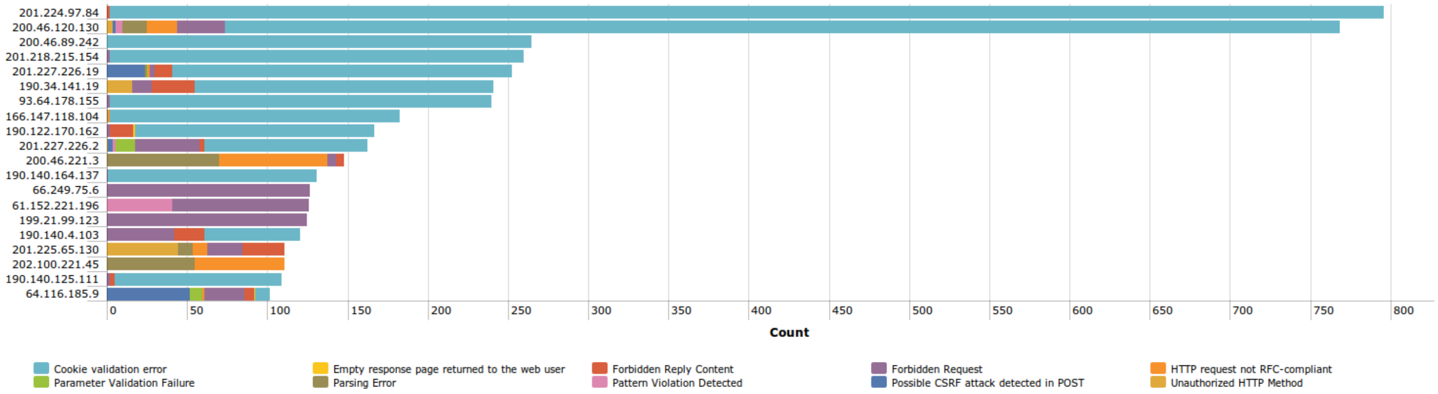
Graph: Top Attacks by Tunnel

This report provides the count of total attacks by tunnel.



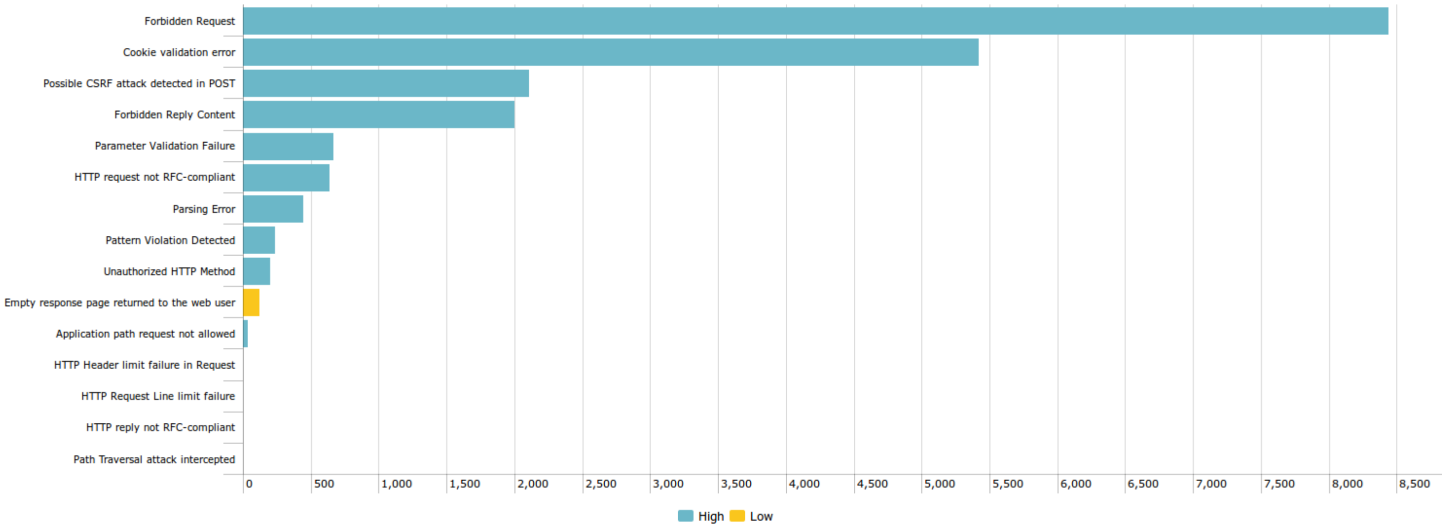
Graph: Top Attacks by Source

This report provides the count of total attacks by source.



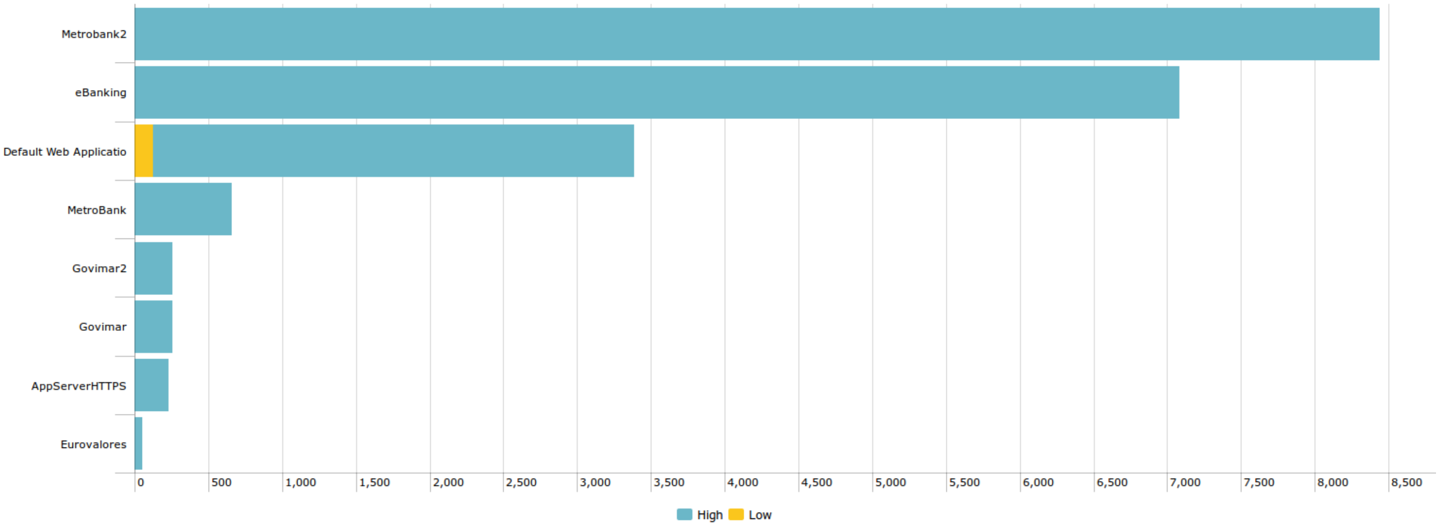
Graph: Attacks by Severity

This report provides the number of attacks by severity.



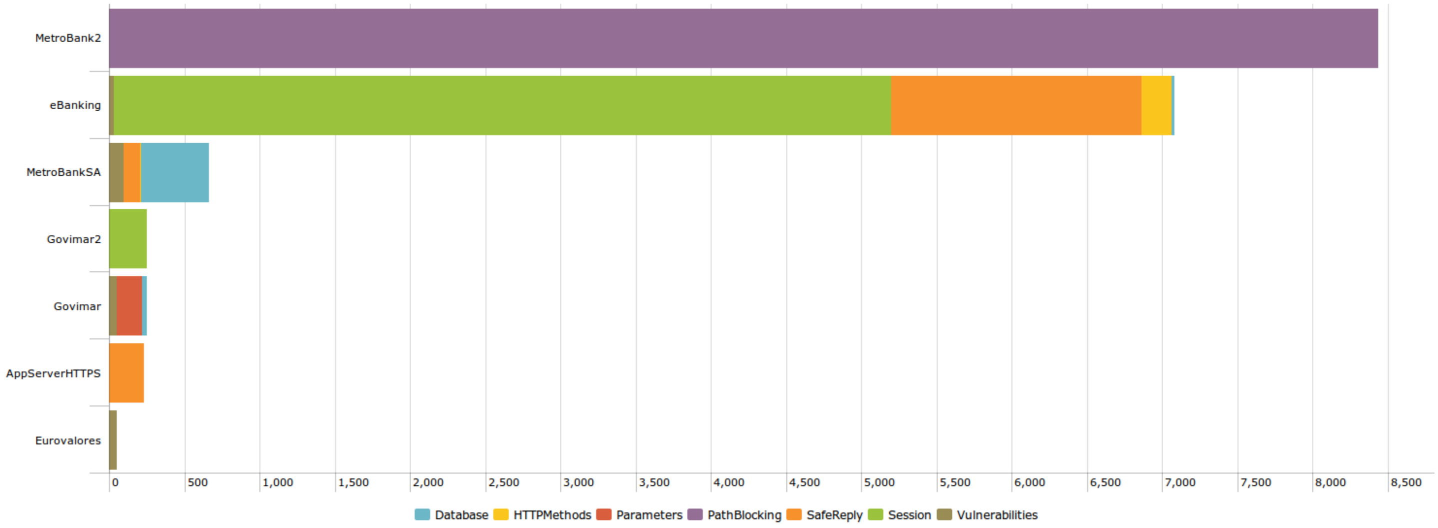
Graph: Web Application by Severity

This report provides the number of attacks on web applications by severity.



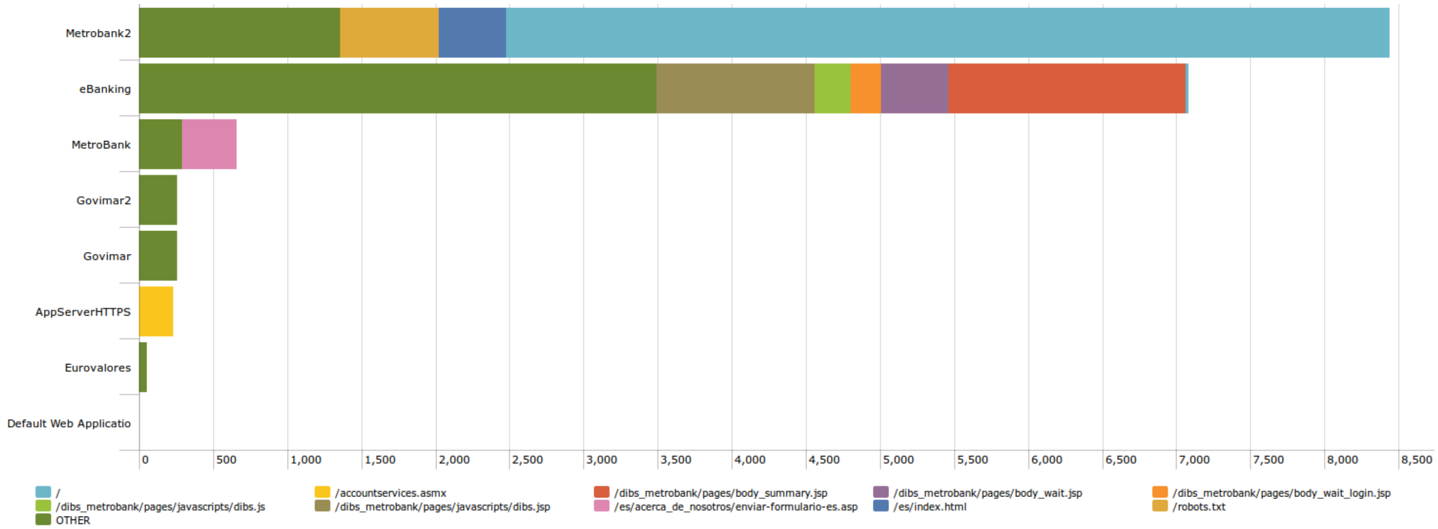
Graph: Tunnel by Object (Category)

This report provides the tunnels by object category. Attacks are grouped into objects (categories).



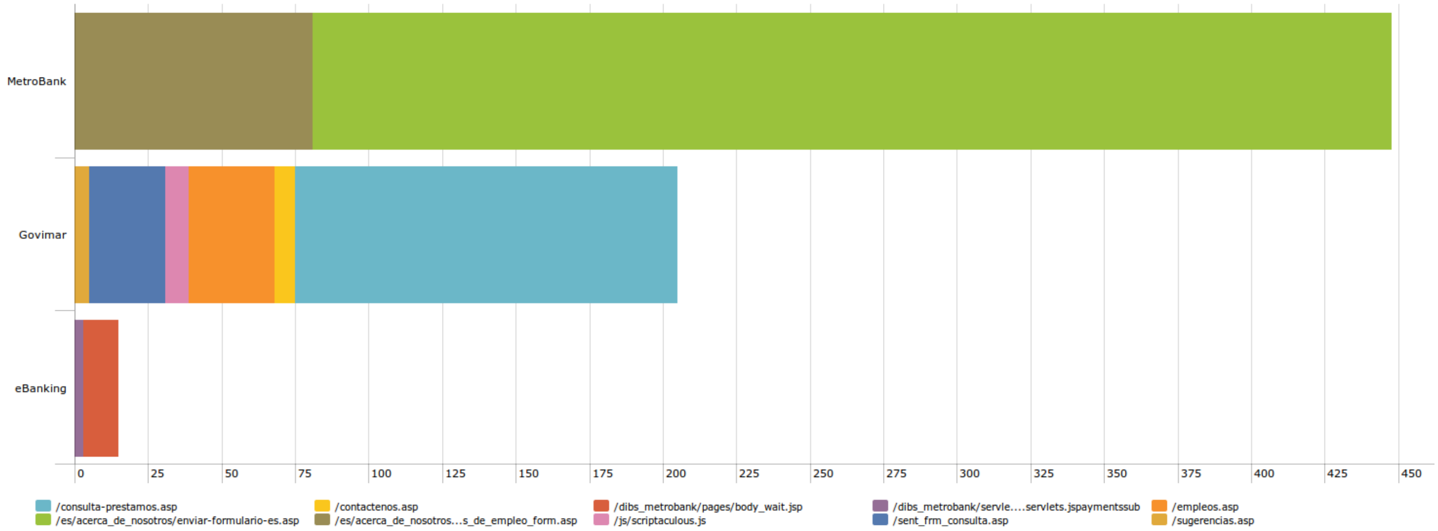
Graph: Tunnel by Object (Category)

This report provides the tunnels by object category. Attacks are grouped into objects (categories).



Graph: Input Validation Violation

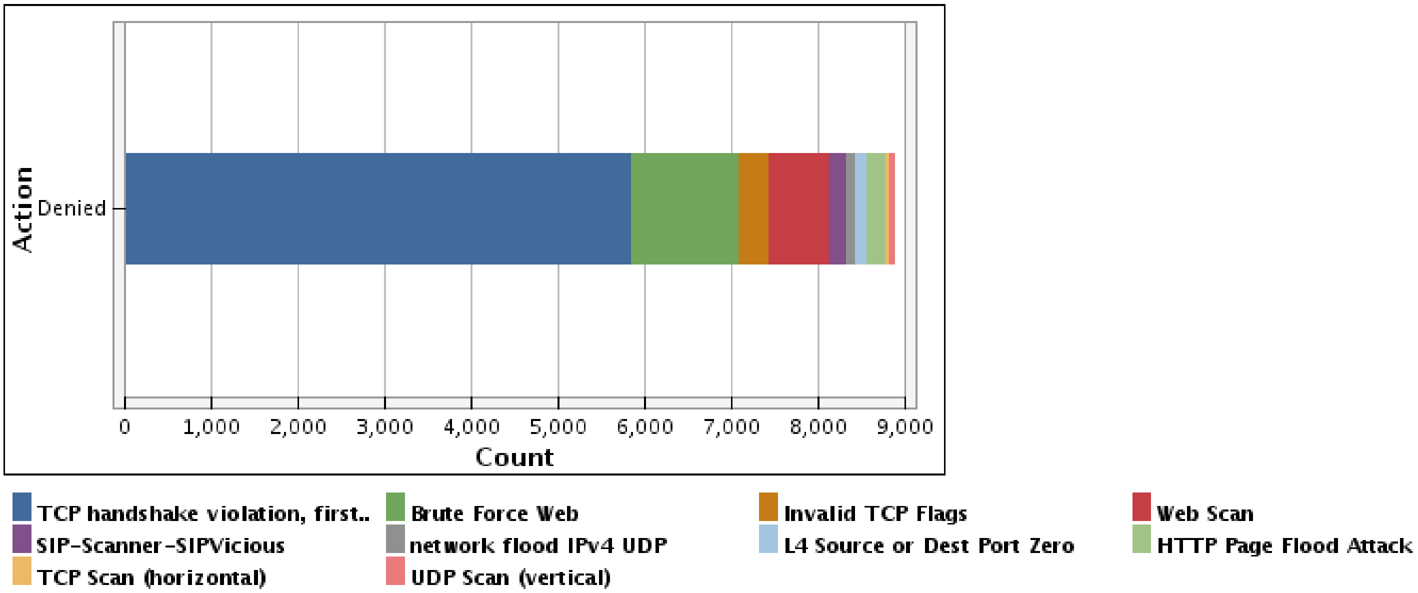
This report shows count of Input Validation Violation attacks for the combination of Web Application Name, and URI.



DefensePro

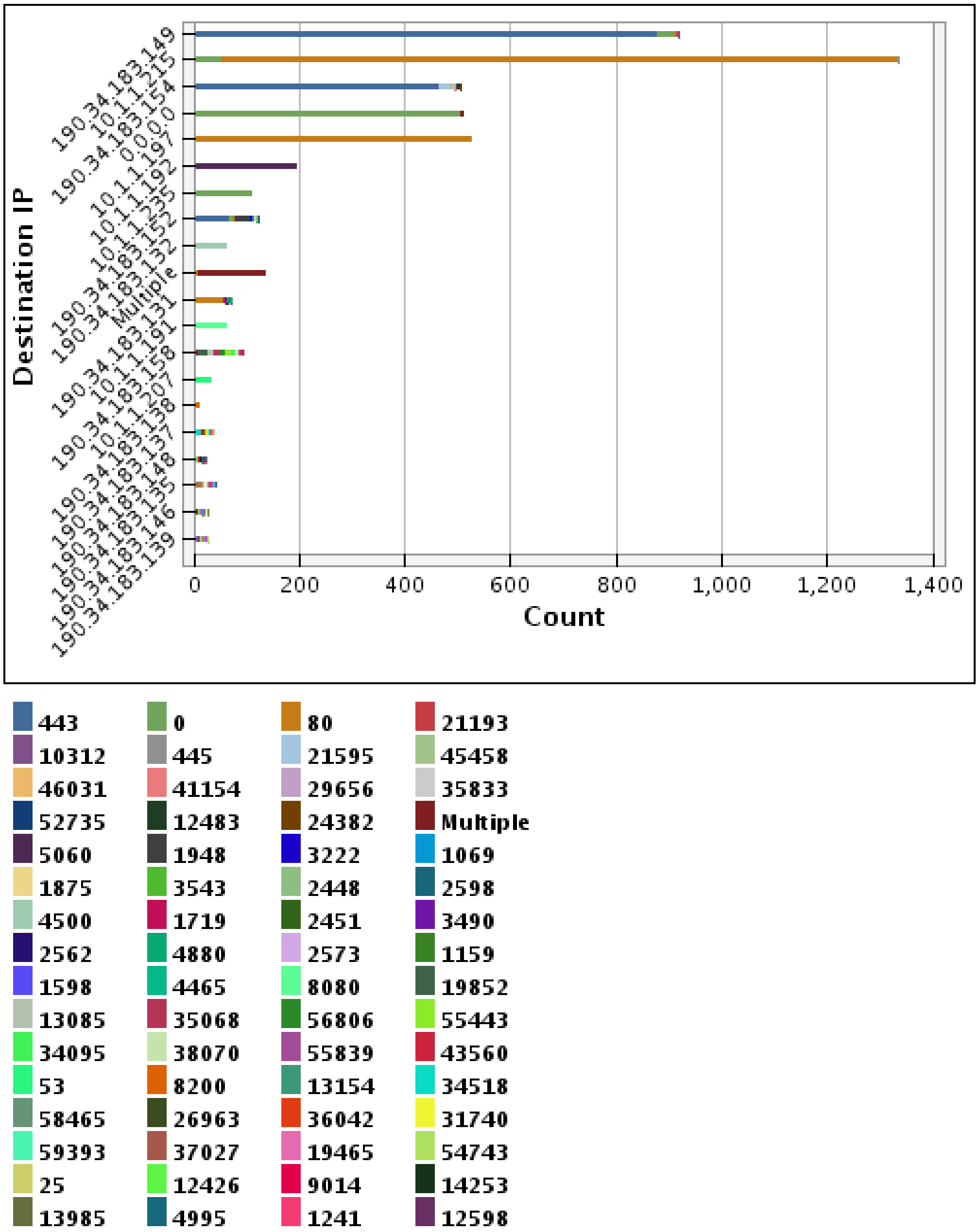
Graph: Attacks Allowed and Denied

This report provides the count of total allowed and denied attacks along with network security rule.



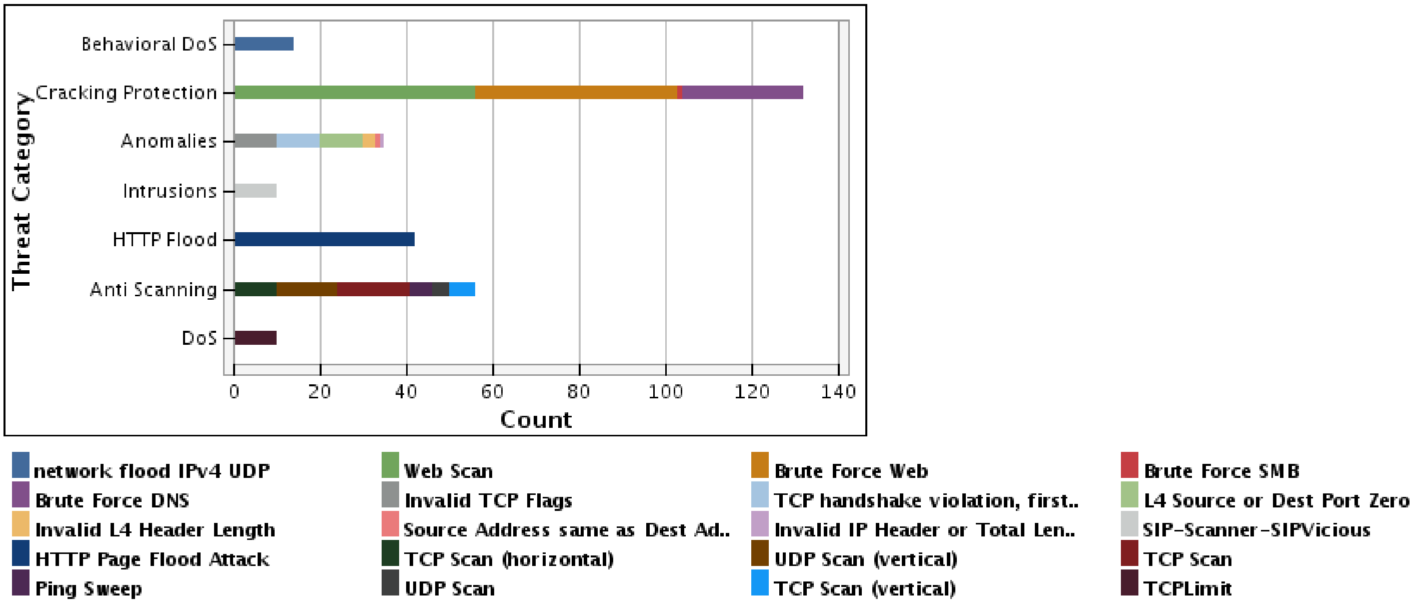
Graph: Attacks by Destination and Port

This report provides information on the total number of attacks that were attempted on which target device and port and for how many times, along with the attack name, network security rule.



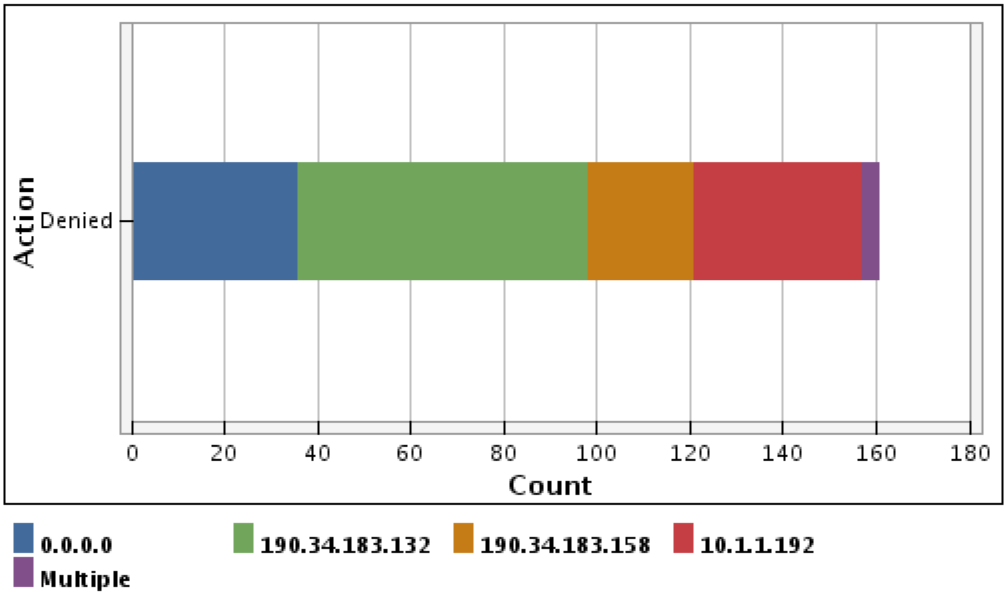
Graph: Attacks By Threat Category

This report lists the attacks per Attack Category, listing the attack name, network security rule.



Graph: Critical Attacks

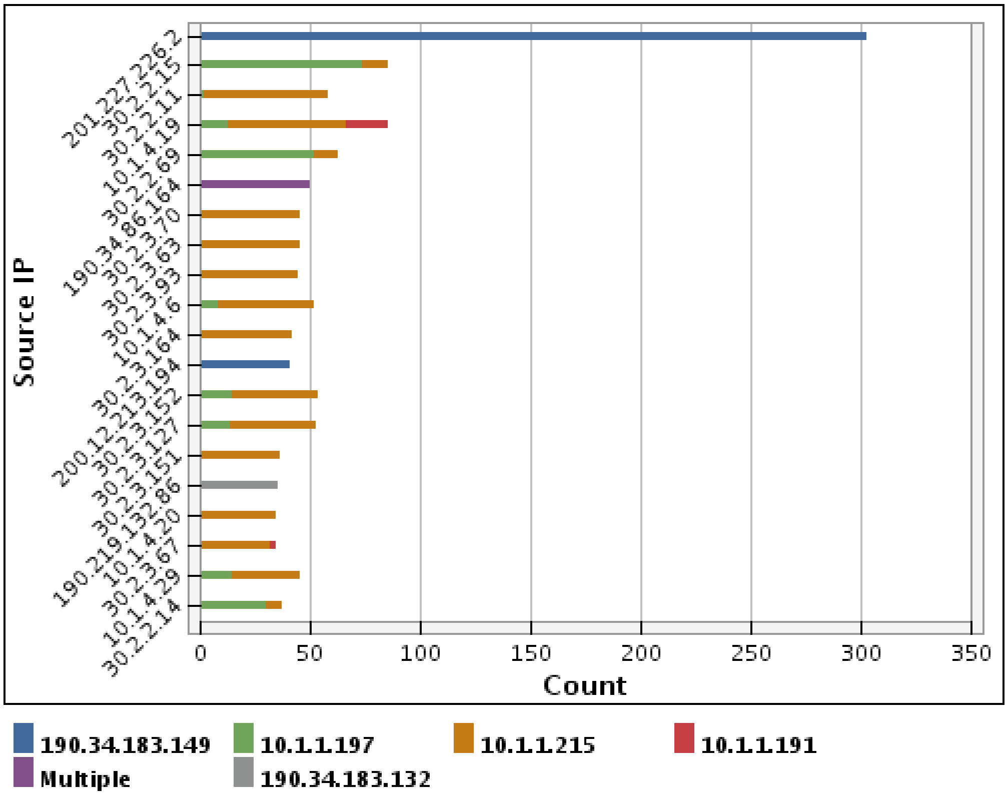
This report provides Critical Attacks information, which includes the destination on which the attack was targeted, the source from where the critical attack originated, port, attack name, network security rule along with the number of times the attack was launched.



NOTE: See Appendix 1 – Critical Attack Sources (WHOIS Information)

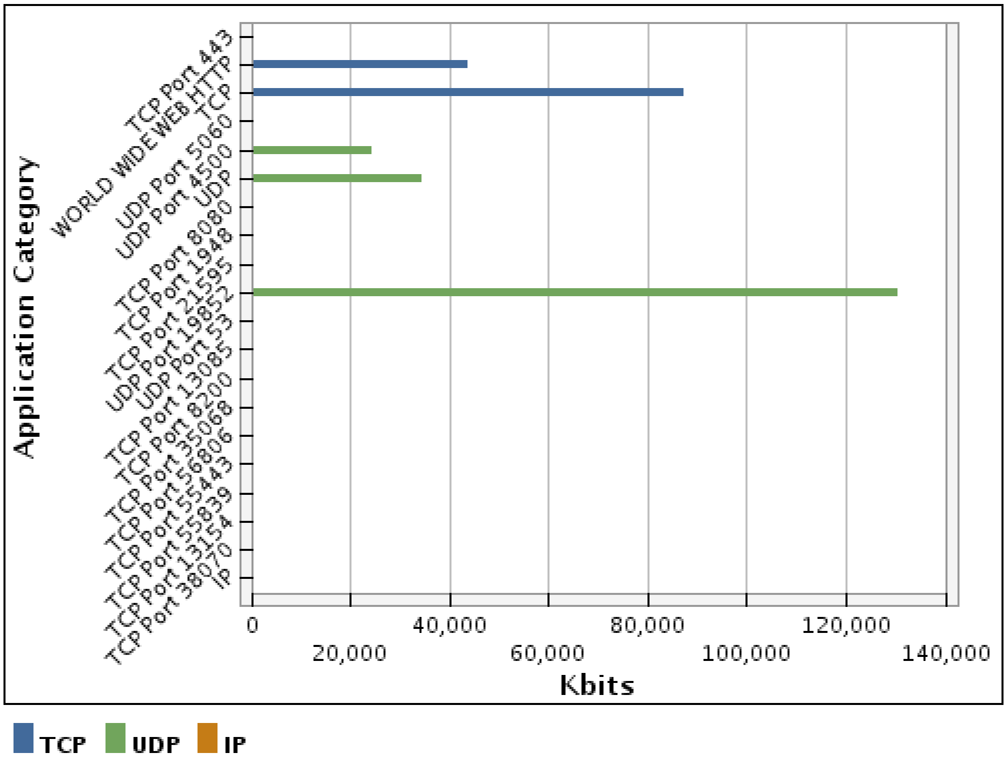
Graph: Top Attack Sources Blocked

This report provides information on the top sources that were blocked on the DP IPS and from where the attacks had originated. This report also shows the destination on which the attack was targeted, its destination port along with the network security rule.



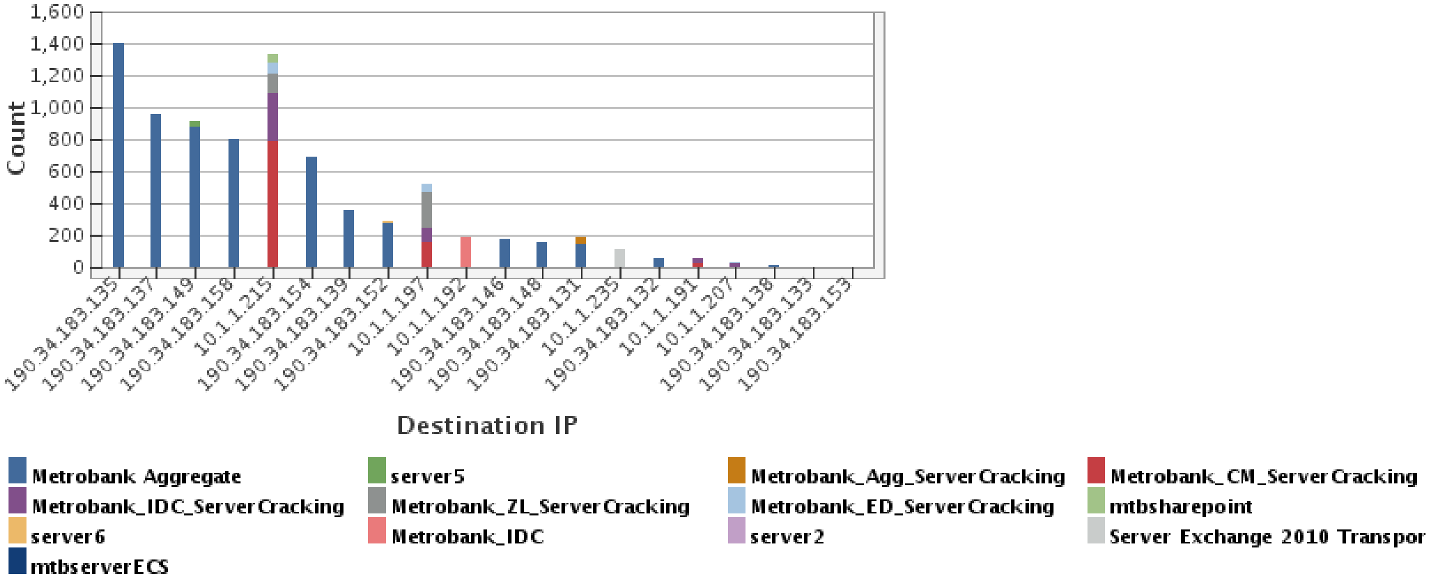
Graph: Top Attacked Applications

This report provides information on the most popular protocol families (or application categories) like web (http, https), e-mail (smtp, pop3)... and their respective child protocols. It also shows the port used by the protocol, the network security rule and the details of number of hits for each protocol family (or application category).



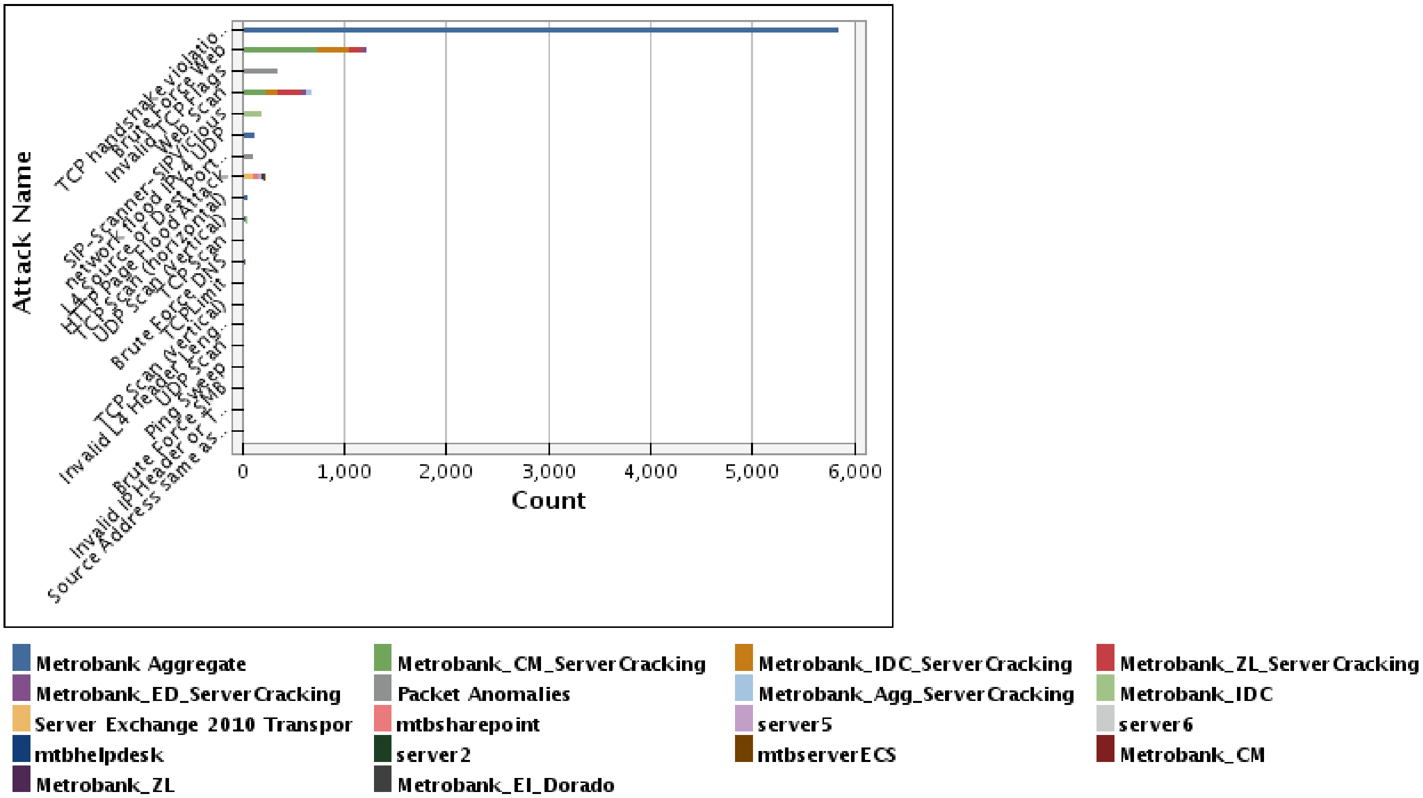
Graph: Top Attacked Destinations

This report provides information on the system IPs, which were the destination of the attacks for most number of times along with the network security rule.



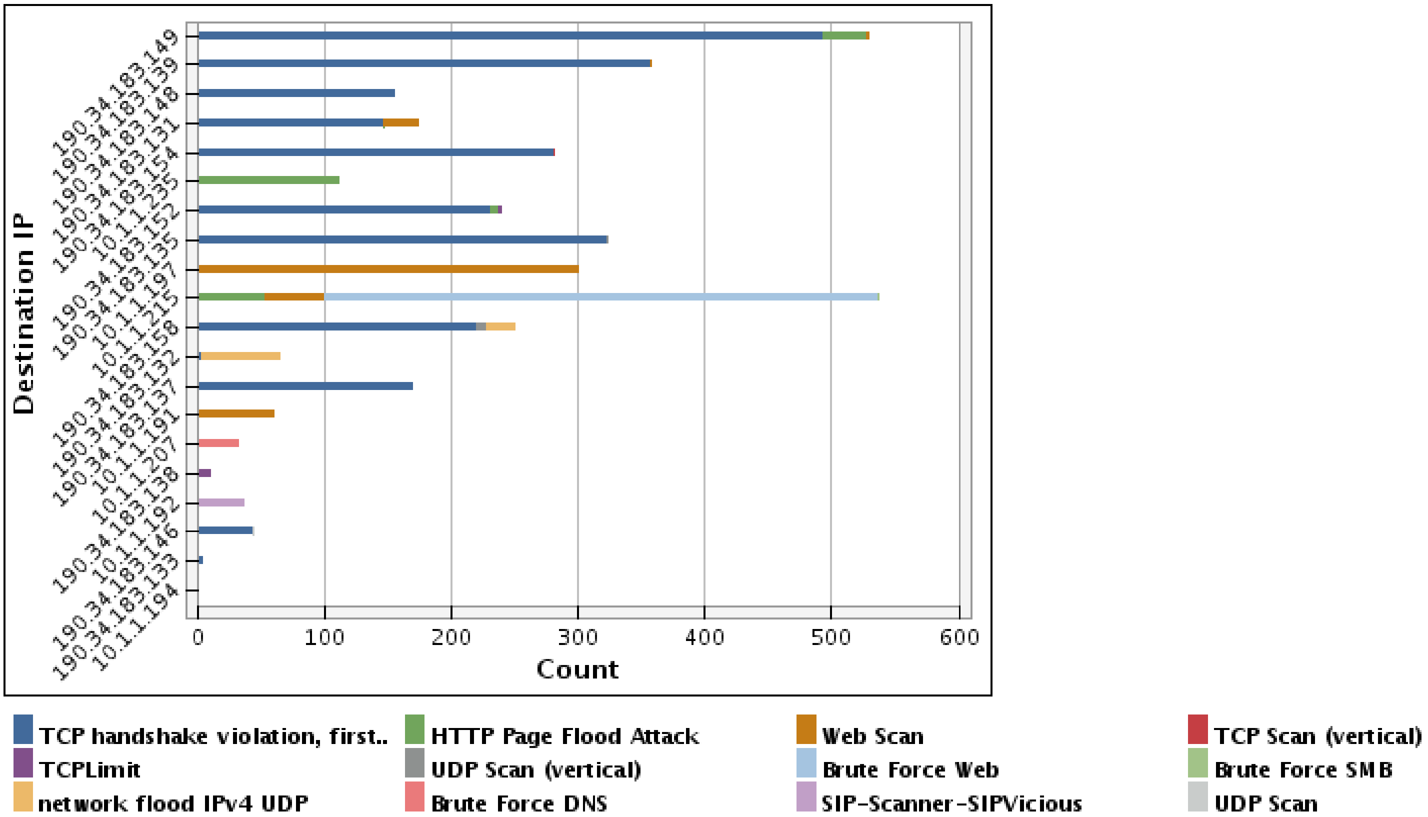
Graph: Top Attacks Blocked

This report provides information on the Top Attacks Blocked, the attack name, network security rule and VLAN and the total number of attacks blocked with this combination.



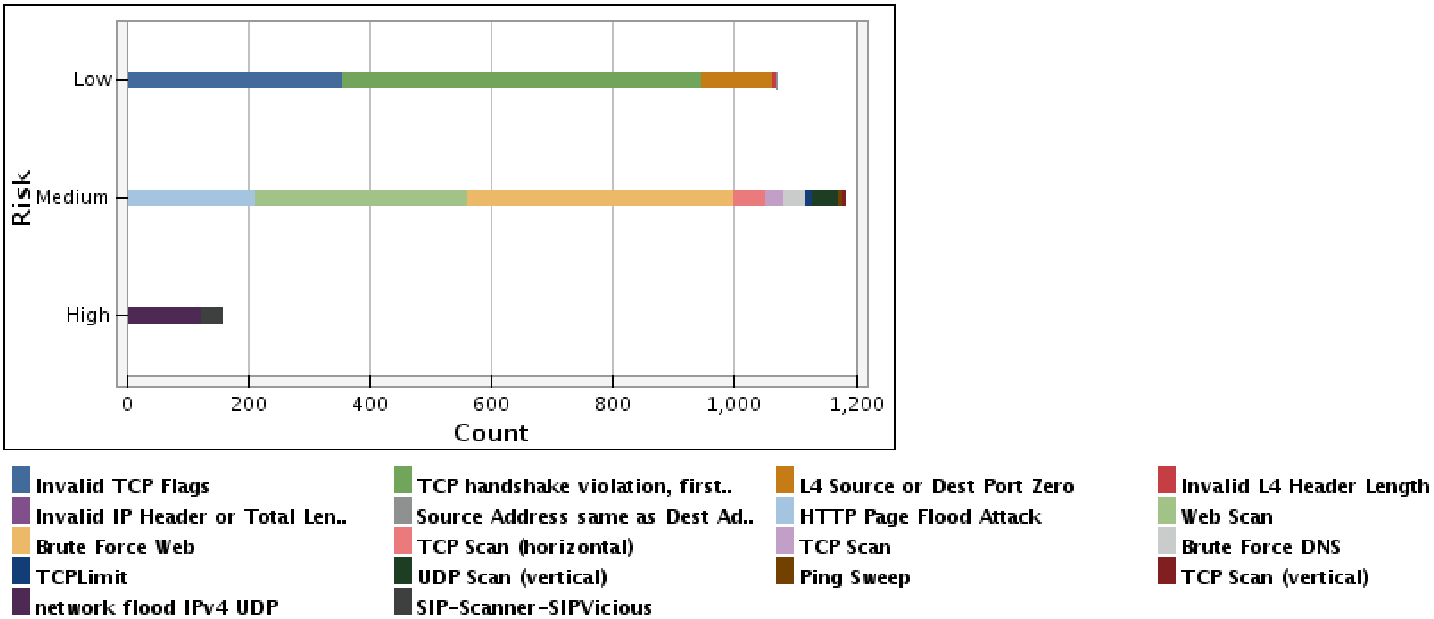
Graph: Top Attacks Blocked by Destination

This report provides information on the top attacks targeted at destinations that were blocked on the DP IPS. In this report the destination on which the attack was targeted, attack name, the source from where the attack had originated, network security rule are shown.



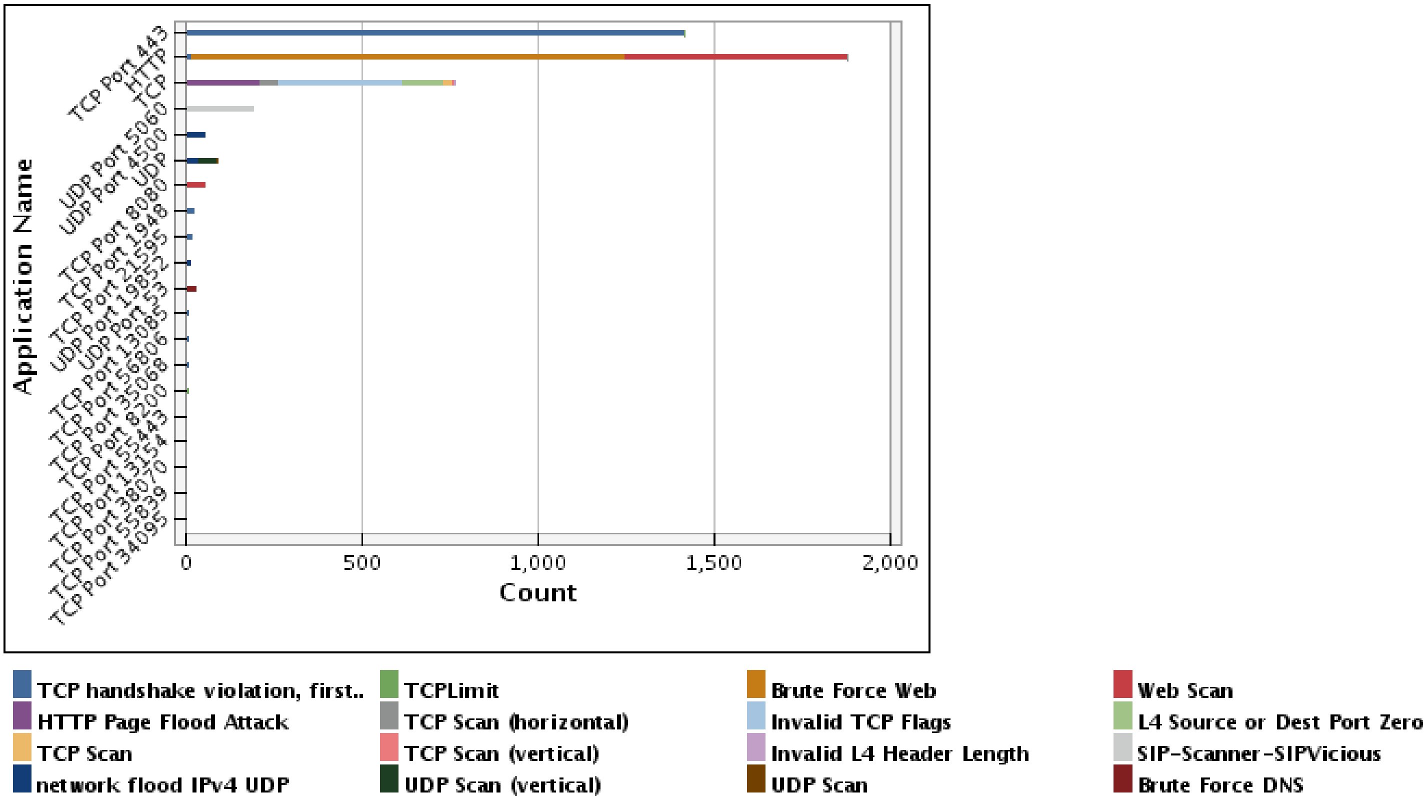
Graph: Top Attacks Blocked By Risk

This report provides information on the attacks, which were blocked on DP IPS based on their risk. In this report the risk of the attack, attack name, source, destination, the destination port, network security rules are shown.



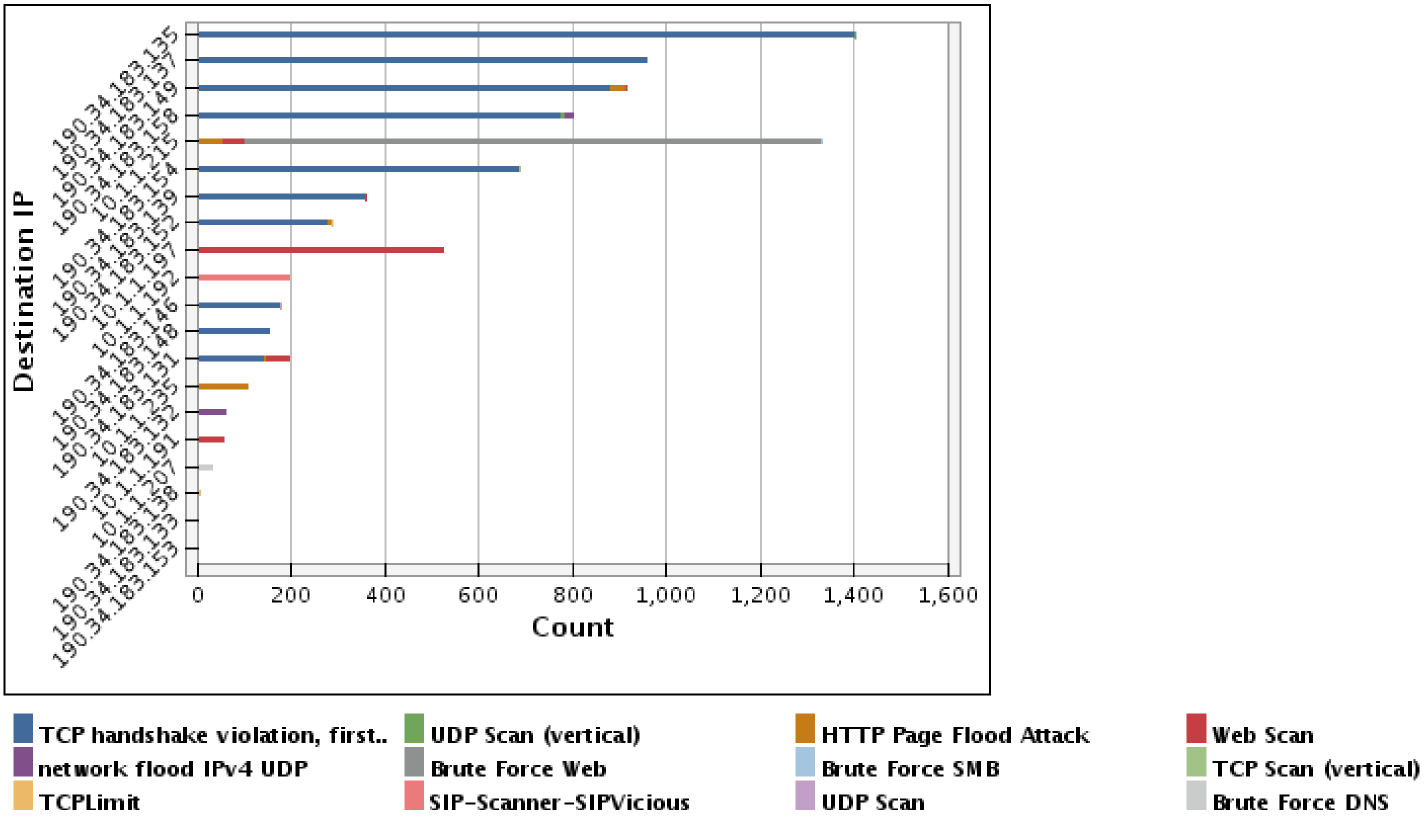
Graph: Top Attacks by Application

This report provides information on the top attacks attempted, categorized by attacks for each source that was the source of attacks along with the attack name, network security rule and the number of attacks that triggered with this combination.



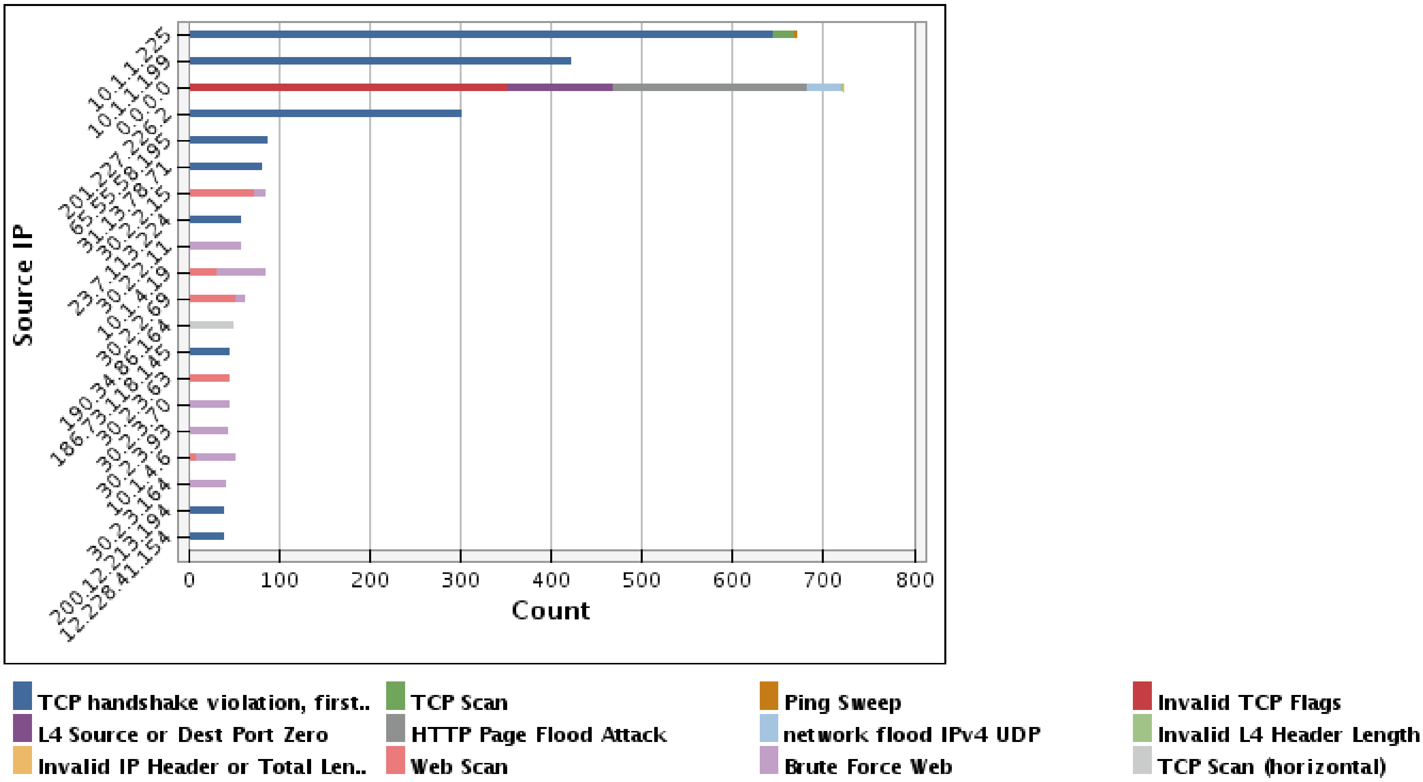
Graph: Top Attacks by Destination

This report provides information on the destination system IPs with most number of attacks. This report also displays the attack name, network security rule and VLAN and the total count of attacks with this combination.



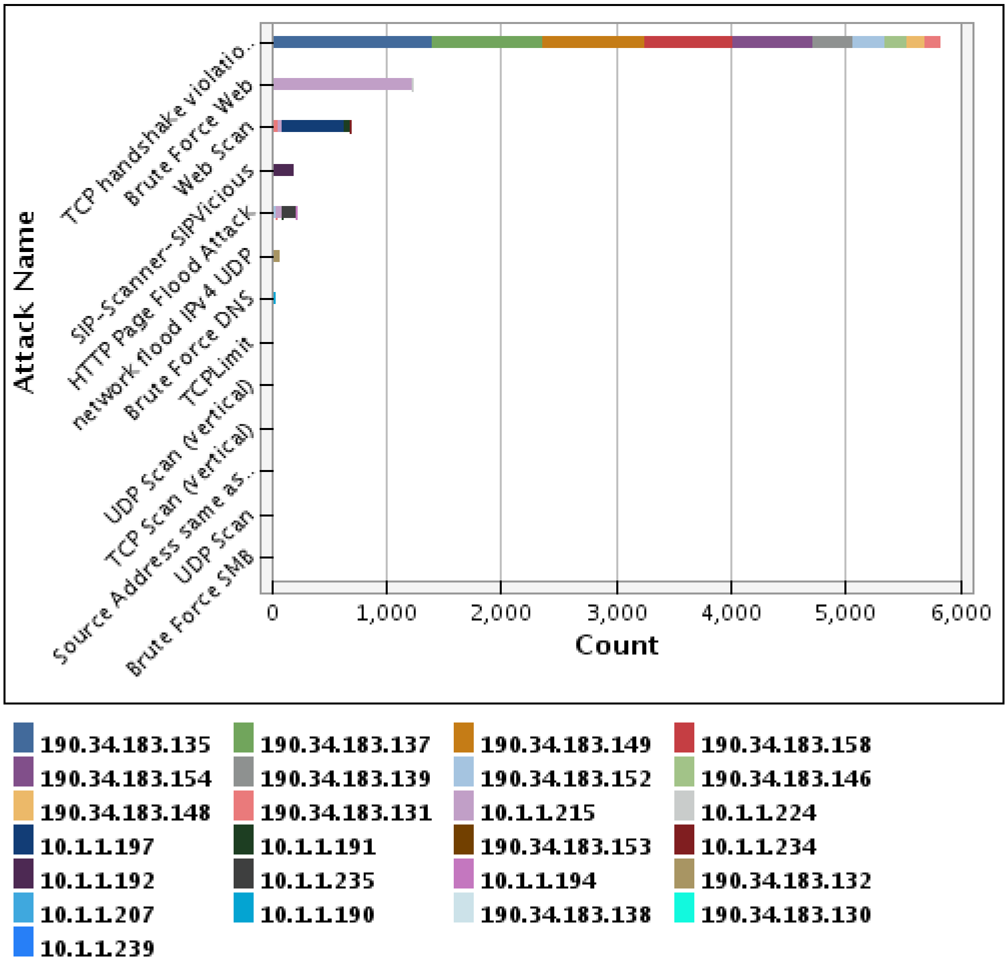
Graph: Top Attacks by Source

This report provides information on the top attacks attempted, categorized by attacks for each source that was the source of attacks along with the attack name, network security rule and the number of attacks that triggered with this combination.



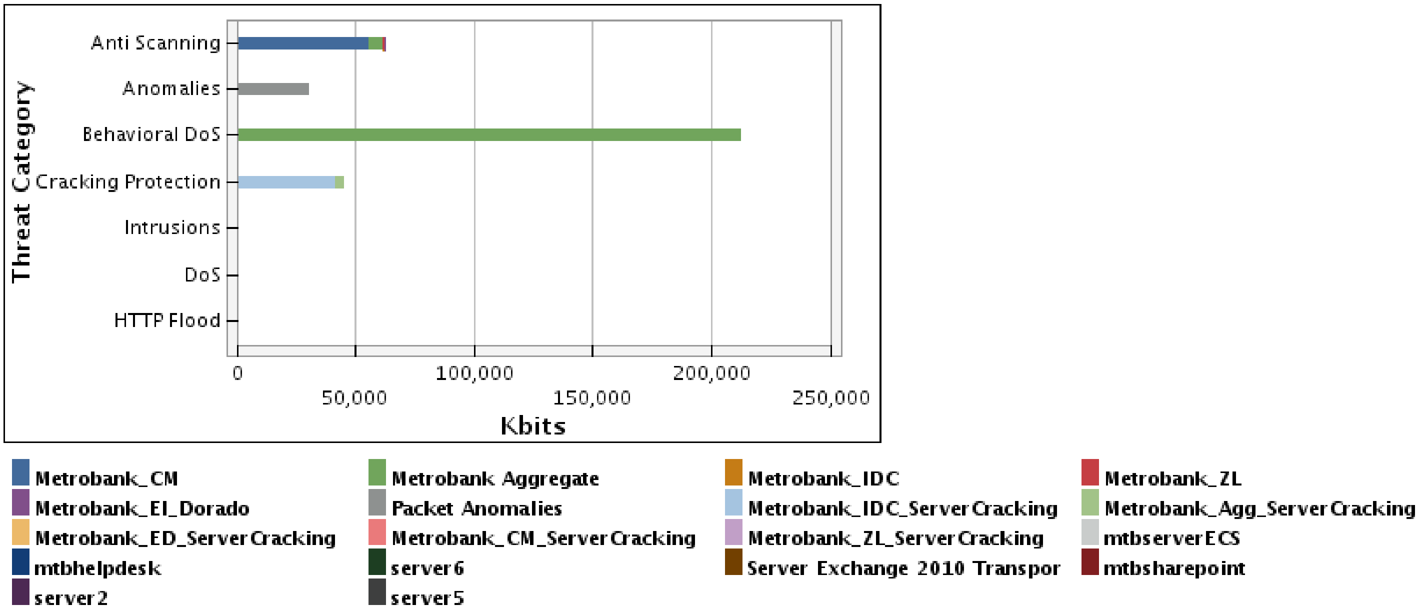
Graph: Top Destinations by Attack

This report provides information on the attacks attempted for the most number of times on the destination protected system IPs along with the network security rule.



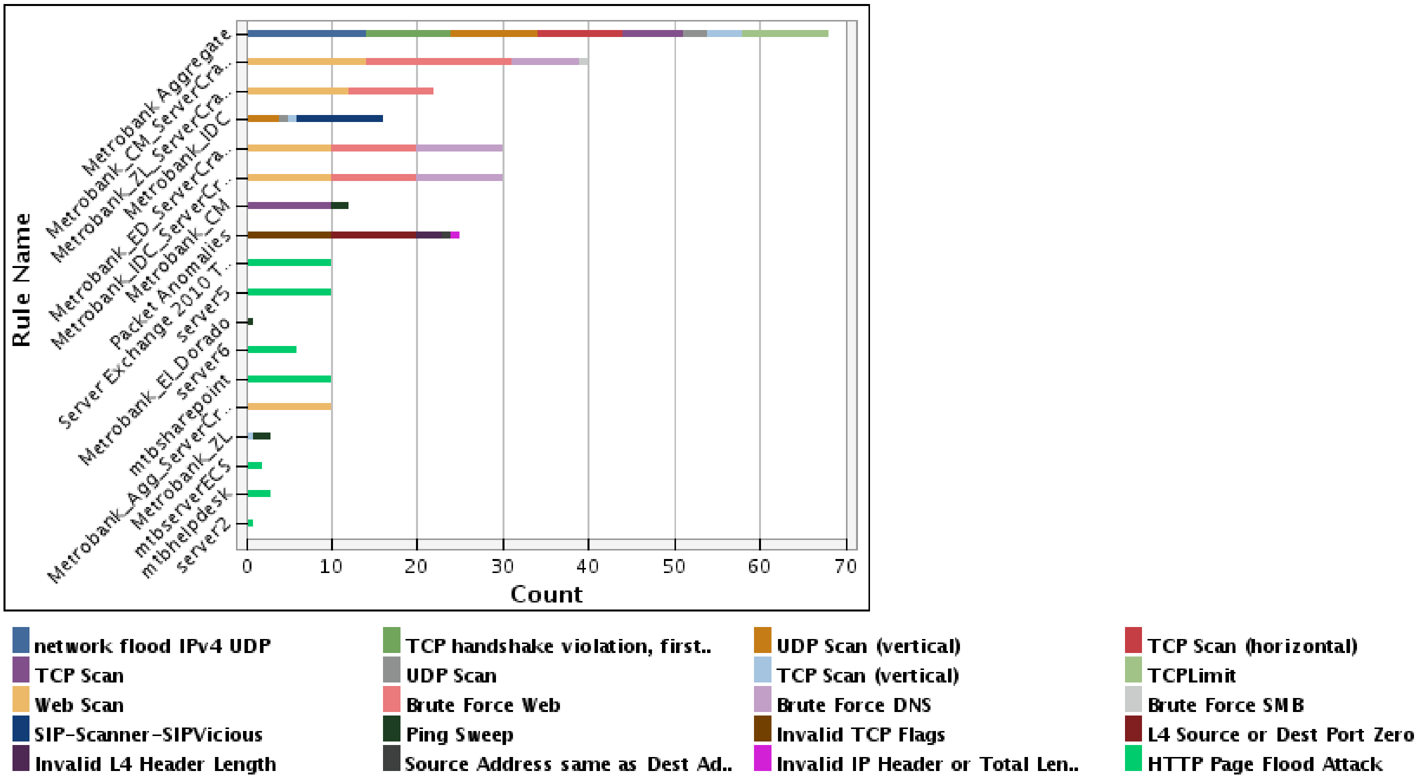
Graph: Attack Categories by Bandwidth

This report shows the attack categories based on the BW of the attacks sharing the same category including Packets and Bits (Kbits). This report also shows the network security rule for each of the attack categories.



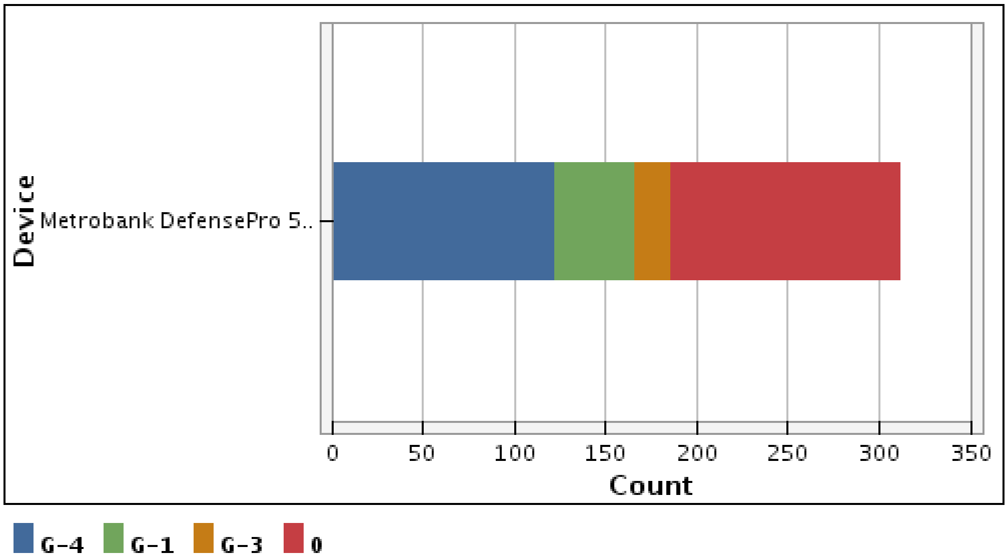
Graph: Attacks by Network Security Rule

This report lists the attacks per network security rule, listing the attack name, Risk and last time stamp.



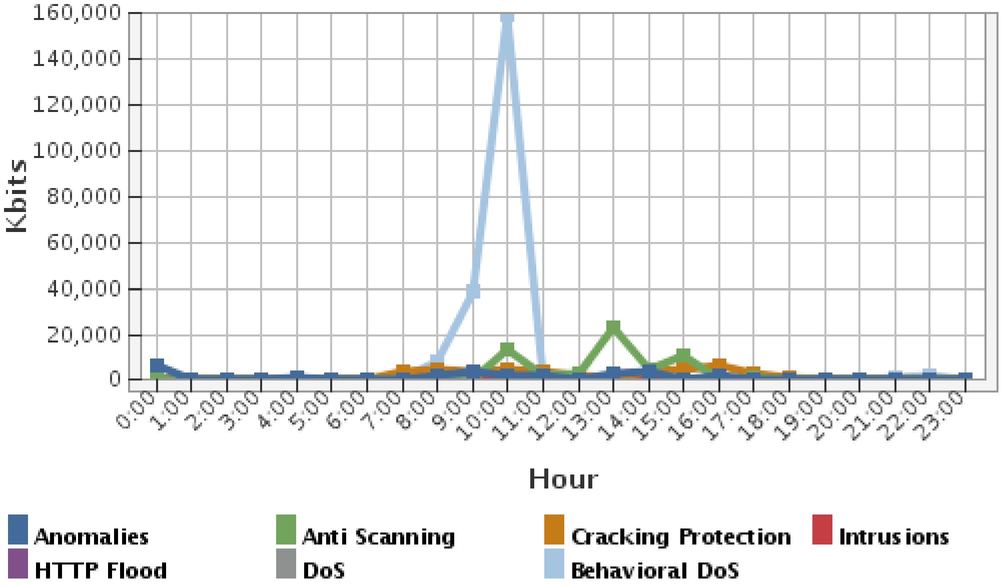
Graph: Attacks by Physical Port (per single IPS device)

This report lists the attacks per physical port.



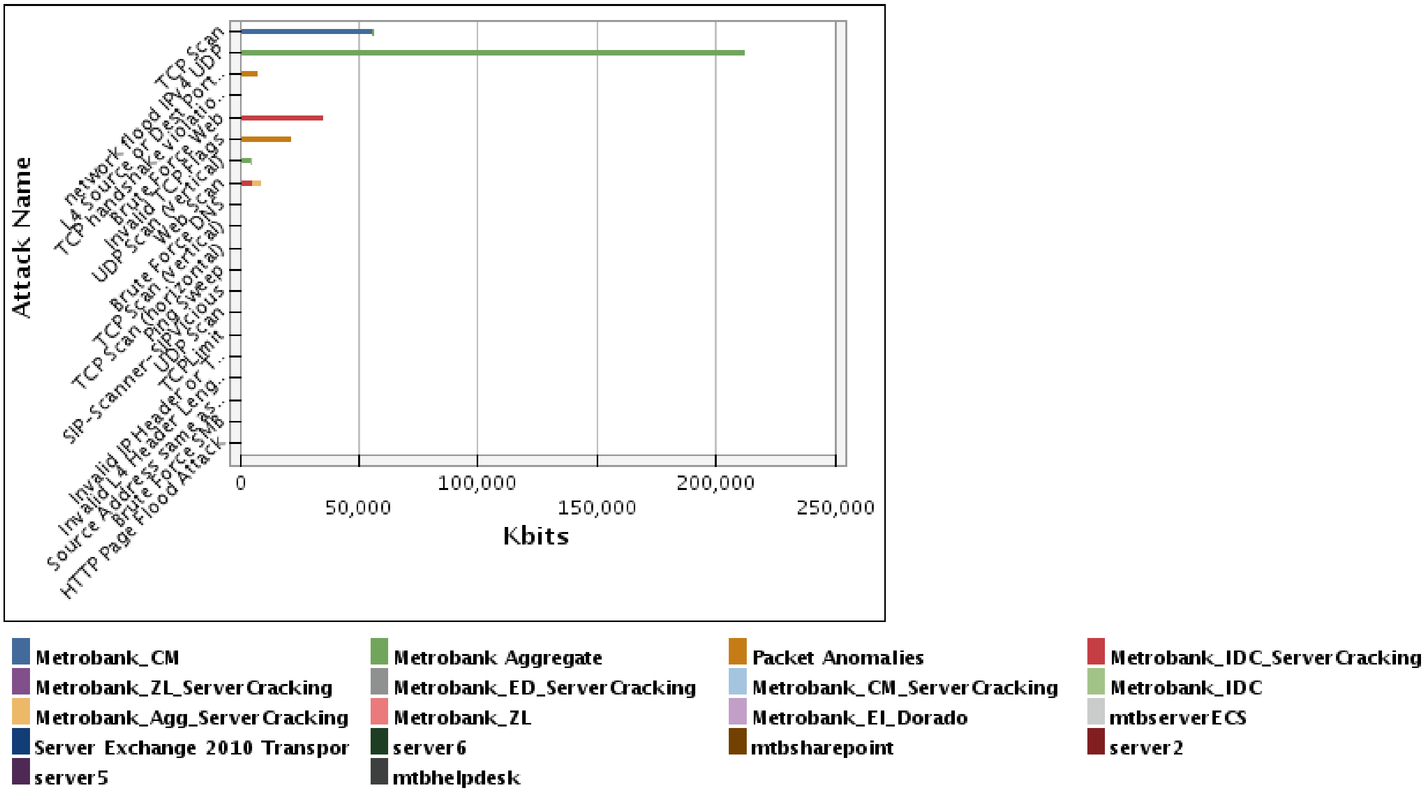
Graph: Bandwidth by Threat Category by Hour of Day

This report shows the most bandwidth (BW) consuming threat categories based on the bandwidth (BW) of the attacks sharing the same threat category including Packets and Bits (Kbits) for each hour of day. This report also shows the network security rule and threat categories.



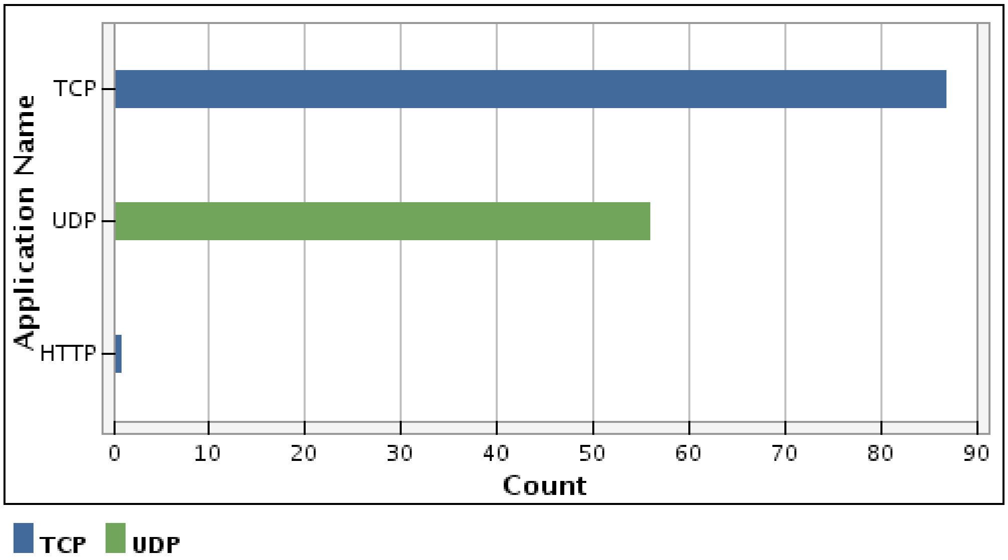
Graph: Top Attacks by Bandwidth

This report shows the most bandwidth (BW) consuming attacks based on the BW of the attack including Packets and Bits (Kbits). This report also shows the network security rule and for each attack.



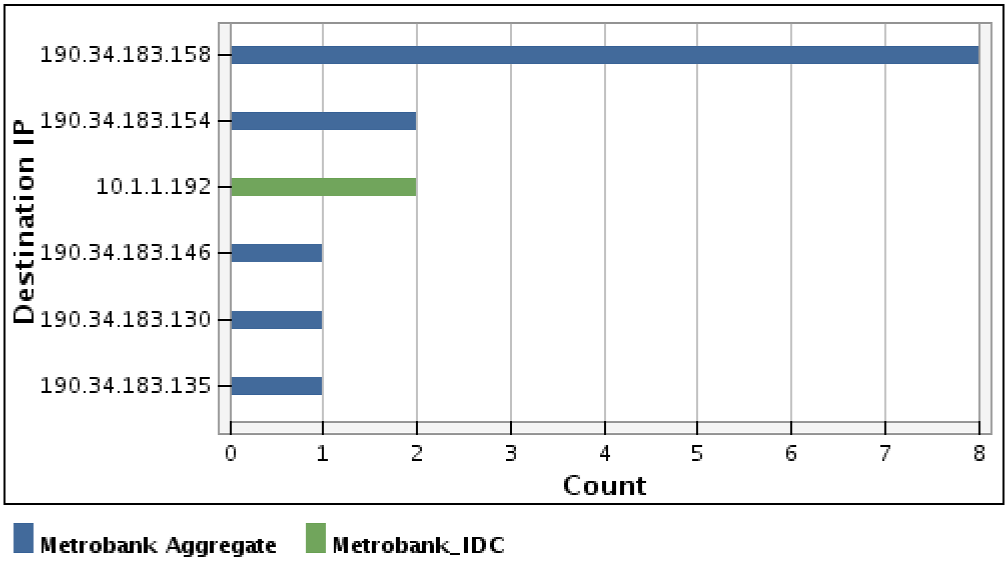
Graph: Top Probed Applications

This report shows historical view of the TOP probed L4 ports (mapped to L7 application name) that were being scanned along with the network security rule.



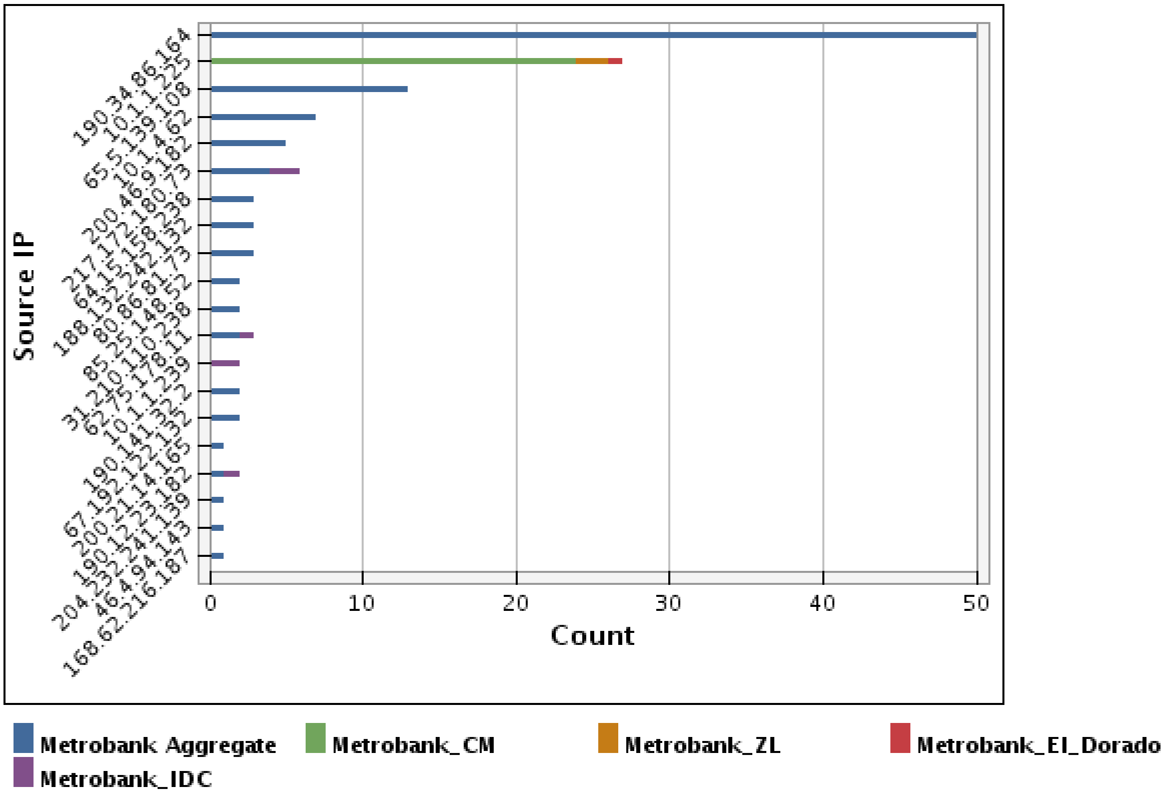
Graph: Top Probed IP Addresses

This report shows historical view of the TOP probed IP addresses that were being scanned along with the network security rule.



Graph: Top Scanners (Source IP Addressed)

This report shows historical view of the TOP source IP addresses that have scanned the network by network scanning activities along with the network security rule.



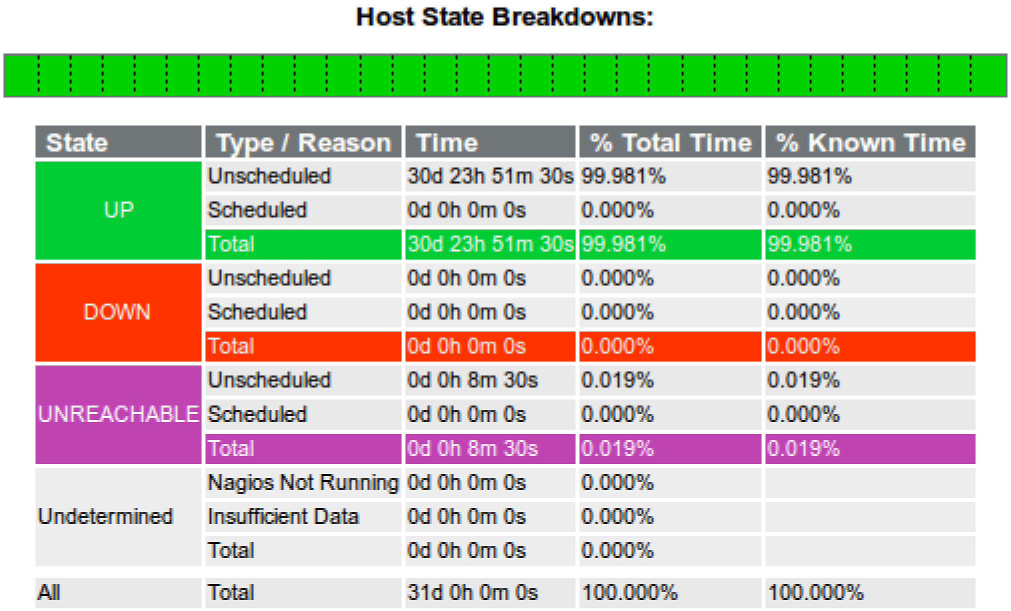
7. Security Operations

The purpose of this section is to highlight the activities performed by GLESEC's Global Operations Center (GOC) including: monitoring availability and performance of equipment under contract, Incident Response, and Change Management activities.

a) Monitoring System Availability

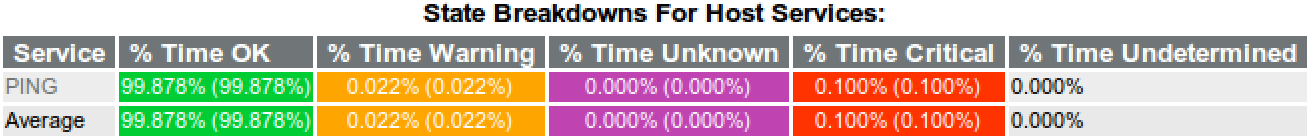
METROBANK AppWall Availability:

The AppWall was considered up and available from the GLESEC GOC to METROBANK **99.981%** during this report period.



Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	30d 23h 51m 30s	99.981%	99.981%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	30d 23h 51m 30s	99.981%	99.981%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 8m 30s	0.019%	0.019%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 8m 30s	0.019%	0.019%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	31d 0h 0m 0s	100.000%	100.000%

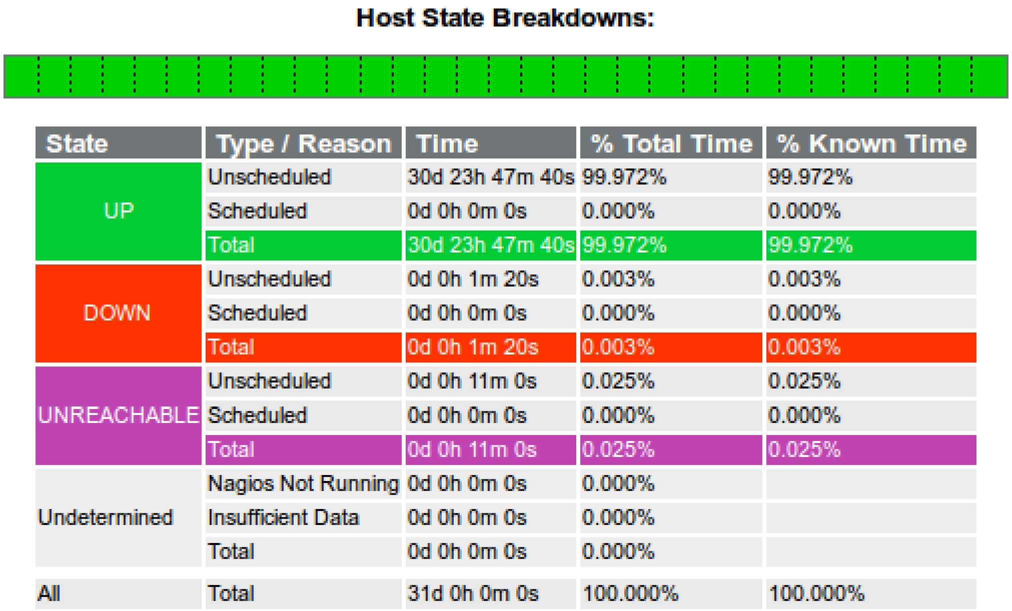


State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.878% (99.878%)	0.022% (0.022%)	0.000% (0.000%)	0.100% (0.100%)	0.000%
Average	99.878% (99.878%)	0.022% (0.022%)	0.000% (0.000%)	0.100% (0.100%)	0.000%

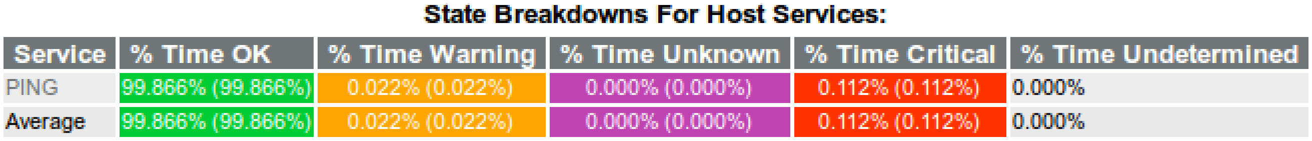
METROBANK DefensePro Availability:

The DefensePro was considered up and available from the GLESEC GOC to METROBANK **99.972%** during this report period.



Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	30d 23h 47m 40s	99.972%	99.972%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	30d 23h 47m 40s	99.972%	99.972%
DOWN	Unscheduled	0d 0h 1m 20s	0.003%	0.003%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 1m 20s	0.003%	0.003%
UNREACHABLE	Unscheduled	0d 0h 11m 0s	0.025%	0.025%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 11m 0s	0.025%	0.025%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	31d 0h 0m 0s	100.000%	100.000%



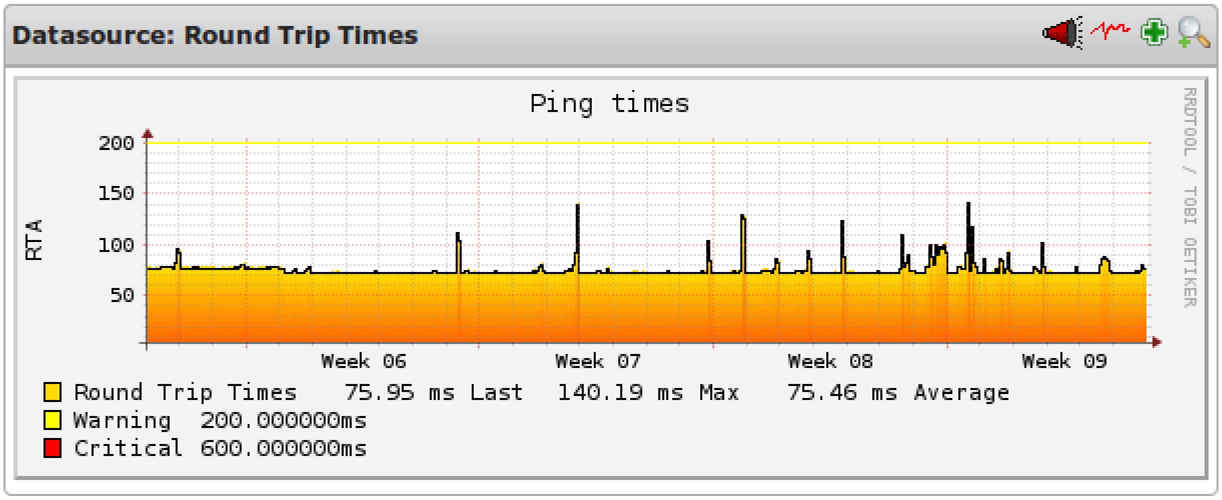
State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.866% (99.866%)	0.022% (0.022%)	0.000% (0.000%)	0.112% (0.112%)	0.000%
Average	99.866% (99.866%)	0.022% (0.022%)	0.000% (0.000%)	0.112% (0.112%)	0.000%

b) Monitoring System Performance

METROBANK AppWall Performance:

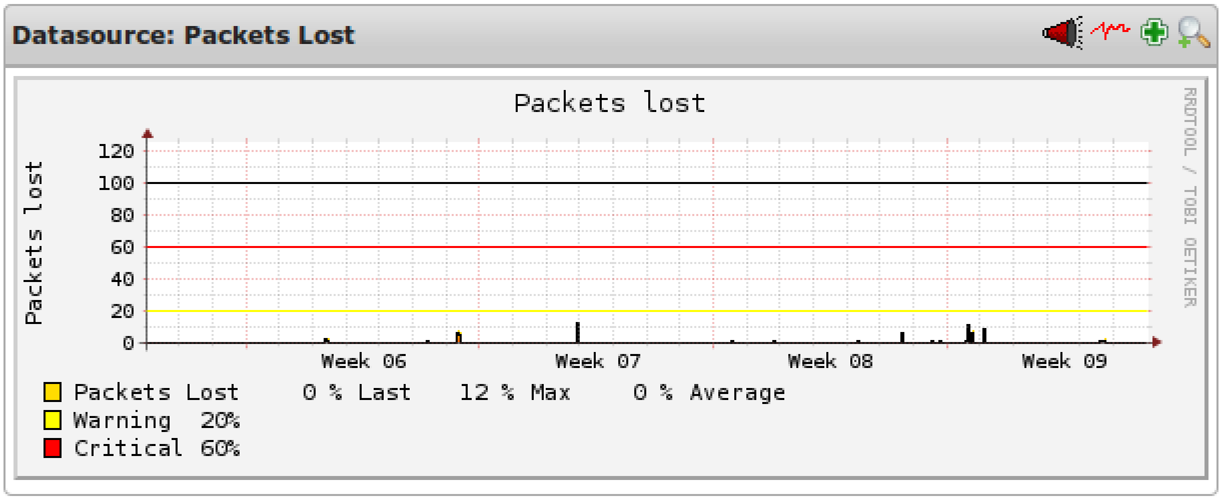
Round trip ping times averaged **75.46** ms from the GLESEC GOC to METROBANK with **0%** average packet loss.



Datasource: Round Trip Times

Ping times

```
□ Round Trip Times   75.95 ms Last  140.19 ms Max   75.46 ms Average
□ Warning  200.000000ms
■ Critical  600.000000ms
```



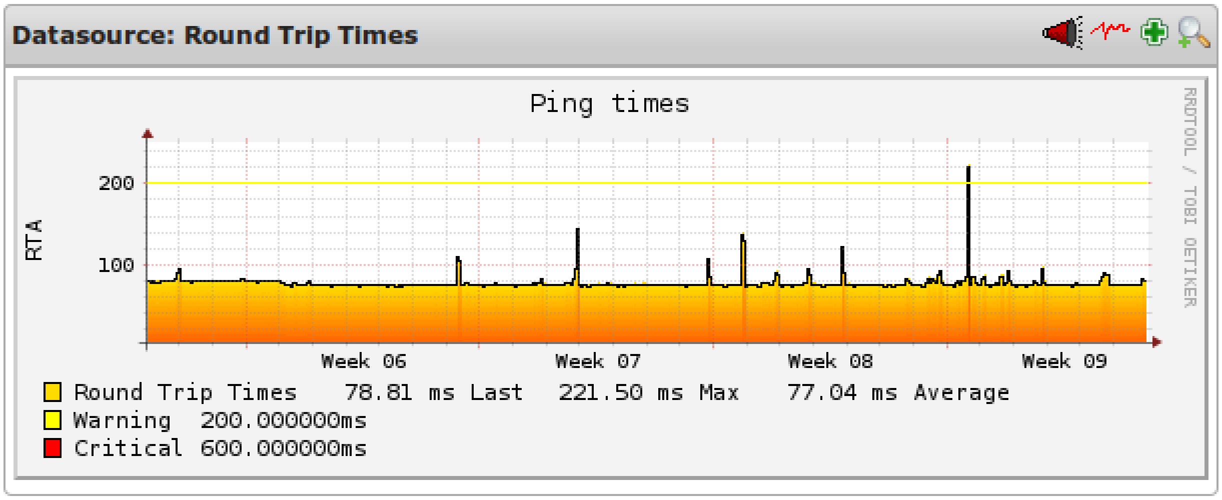
Datasource: Packets Lost

Packets lost

```
□ Packets Lost     0 % Last    12 % Max     0 % Average
□ Warning  20%
■ Critical  60%
```

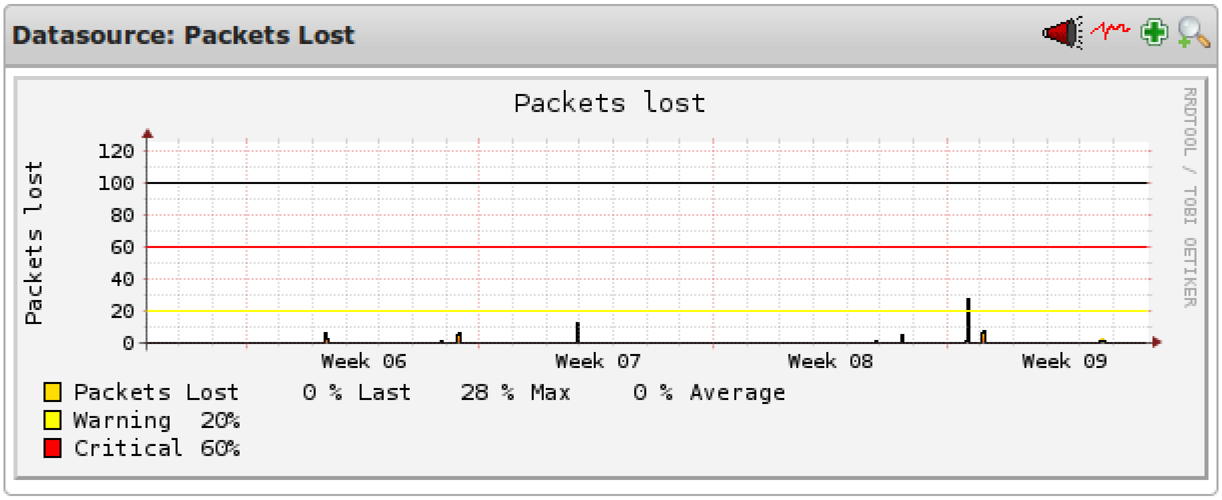
METROBANK DefensePro Performance:

Round trip ping times averaged **77.04** ms from the GLESEC GOC to METROBANK with **0%** average packet loss.



Datasource: Round Trip Times

```
🟨 Round Trip Times    78.81 ms Last    221.50 ms Max    77.04 ms Average
🟨 Warning  200.000000ms
🟥 Critical  600.000000ms
```



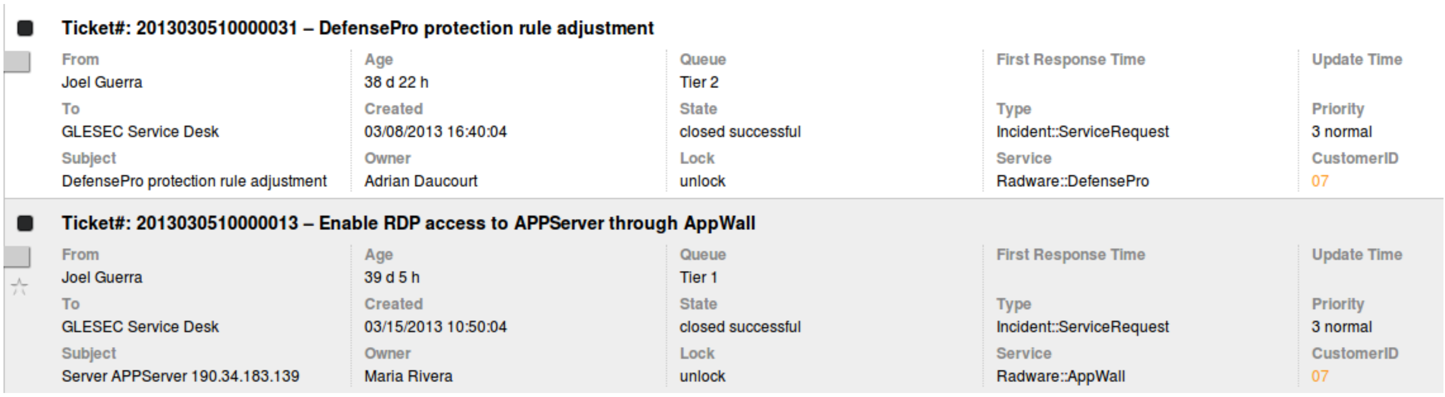
Datasource: Packets Lost

```
🟨 Packets Lost     0 % Last     28 % Max     0 % Average
🟨 Warning  20%
🟥 Critical  60%
```

c) Change management procedures

METROBANK Change Management:

Two Change Management procedures occurred during the last report period. One to adjust the protection rules for the DefensePro platform, and the other to enable RDP access to the AppServer for a contractor through the Appwall at METROBANK.



Ticket#: 2013030510000031 – DefensePro protection rule adjustment

From	Age	Queue	First Response Time	Update Time
Joel Guerra	38 d 22 h	Tier 2		
To	Created	State	Type	Priority
GLESEC Service Desk	03/08/2013 16:40:04	closed successful	Incident::ServiceRequest	3 normal
Subject	Owner	Lock	Service	CustomerID
DefensePro protection rule adjustment	Adrian Daucourt	unlock	Radware::DefensePro	07

Ticket#: 2013030510000013 – Enable RDP access to APPServer through AppWall

From	Age	Queue	First Response Time	Update Time
Joel Guerra	39 d 5 h	Tier 1		
To	Created	State	Type	Priority
GLESEC Service Desk	03/15/2013 10:50:04	closed successful	Incident::ServiceRequest	3 normal
Subject	Owner	Lock	Service	CustomerID
Server APPServer 190.34.183.139	Maria Rivera	unlock	Radware::AppWall	07

d) Incident Response procedures

METROBANK Incident Report: N/A

8. Appendix 1 – Critical Attack Sources (WHOIS Information)

This section provides additional WHOIS detail for the Graph: Critical Attacks

NetRange: 108.0.0.0 - 108.57.255.255

```
CIDR:          108.48.0.0/13, 108.56.0.0/15, 108.32.0.0/12, 108.0.0.0/11
OriginAS:
NetName:        VIS-BLOCK
NetHandle:      NET-108-0-0-0-1
Parent:         NET-108-0-0-0-0
NetType:        Direct Allocation
RegDate:        2009-06-05
Updated:        2012-03-02
Ref:           http://whois.arin.net/rest/net/NET-108-0-0-0-1
OrgName:        Verizon Online LLC
OrgId:         VRIS
Address:        22001 Loudoun County Parkway
City:          Ashburn
StateProv:      VA
PostalCode:     20147
Country:        US
RegDate:
Updated:        2010-08-17
Ref:           http://whois.arin.net/rest/org/VRIS
OrgTechHandle: ZV20-ARIN
OrgTechName:   Verizon Internet Services
OrgTechPhone:  800-243-6994
OrgTechEmail:  IPMGMT-SWIP@gnilink.net
OrgTechRef:    http://whois.arin.net/rest/poc/ZV20-ARIN
OrgAbuseHandle: VISAB-ARIN
OrgAbuseName:   VIS Abuse
OrgAbusePhone:  +1-214-513-6711
OrgAbuseEmail:  security@verizon.net
OrgAbuseRef:    http://whois.arin.net/rest/poc/VISAB-ARIN
inetnum:        109.169.86.0 - 109.169.87.255
netname:        ThrustVPS_PT
descr:         Thrust::VPS
country:        GB
admin-c:        AR9893-RIPE
tech-c:        AR9893-RIPE
status:        ASSIGNED PA
mnt-by:         RAPIDSWITCH-MNT
person:         Abuse Robot
address:        iomart Hosting Ltd t/a ThrustVPS
address:        Spectrum House
address:        Clivemont Road
address:        Maidenhead
address:        SL6 7FW
phone:          +44 (0) 1753 471 040
nic-hdl:       AR9893-RIPE
mnt-by:         RAPIDSWITCH-MNT
route:         109.169.64.0/19
descr:         Iomart Hosting Ltd
origin:        AS20860
mnt-by:         GB10488-RIPE-MNT
mnt-by:         RAPIDSWITCH-MNT
```

NetRange: 173.242.112.0 - 173.242.127.255

```
CIDR:          173.242.112.0/20
```

```
OriginAS:       AS46664
NetName:        VOLUMEDRIVE
NetHandle:      NET-173-242-112-0-1
Parent:         NET-173-0-0-0-0
NetType:        Direct Allocation
Comment:        http://www.volumedrive.com
RegDate:        2010-05-06
Updated:        2012-03-02
Ref:            http://whois.arin.net/rest/net/NET-173-242-112-0-1
OrgName:        VolumeDrive
OrgId:          VOLUM-2
Address:        1143 Northern Blvd
City:           Clarks Summit
StateProv:      PA
PostalCode:     18411
Country:        US
RegDate:        2008-08-26
Updated:        2011-09-24
Ref:            http://whois.arin.net/rest/org/VOLUM-2
OrgTechHandle: VOLUM1-ARIN
OrgTechName:   VolumeDrive POC
OrgTechPhone:  +1-862-266-1083
OrgTechEmail:  info@volumedrive.com
OrgTechRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
OrgAbuseHandle: VOLUM1-ARIN
OrgAbuseName:   VolumeDrive POC
OrgAbusePhone:  +1-862-266-1083
OrgAbuseEmail:  info@volumedrive.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
RNOCHandle: VOLUM-ARIN
RNOCName:   VolumeDrive
RNOCPhone:  +1-862-266-1083
RNOCEmail:  info@volumedrive.com
RNOCRef:    http://whois.arin.net/rest/poc/VOLUM-ARIN
RAbuseHandle: VOLUM-ARIN
RAbuseName:   VolumeDrive
RAbusePhone:  +1-862-266-1083
RAbuseEmail:  info@volumedrive.com
RAbuseRef:    http://whois.arin.net/rest/poc/VOLUM-ARIN
RTechHandle: VOLUM1-ARIN
RTechName:   VolumeDrive POC
RTechPhone:  +1-862-266-1083
RTechEmail:  info@volumedrive.com
RTechRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
```

NetRange: 173.242.112.0 - 173.242.127.255

```
CIDR:           173.242.112.0/20
OriginAS:       AS46664
NetName:        VOLUMEDRIVE
NetHandle:      NET-173-242-112-0-1
Parent:         NET-173-0-0-0-0
NetType:        Direct Allocation
Comment:        http://www.volumedrive.com
RegDate:        2010-05-06
Updated:        2012-03-02
Ref:            http://whois.arin.net/rest/net/NET-173-242-112-0-1
OrgName:        VolumeDrive
OrgId:          VOLUM-2
Address:        1143 Northern Blvd
City:           Clarks Summit
StateProv:      PA
```

```
PostalCode:     18411
Country:        US
RegDate:        2008-08-26
Updated:        2011-09-24
Ref:            http://whois.arin.net/rest/org/VOLUM-2
OrgAbuseHandle: VOLUM1-ARIN
OrgAbuseName:   VolumeDrive POC
OrgAbusePhone:  +1-862-266-1083
OrgAbuseEmail:  info@volumedrive.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
OrgTechHandle: VOLUM1-ARIN
OrgTechName:   VolumeDrive POC
OrgTechPhone:  +1-862-266-1083
OrgTechEmail:  info@volumedrive.com
OrgTechRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
RAbuseHandle: VOLUM-ARIN
RAbuseName:   VolumeDrive
RAbusePhone:  +1-862-266-1083
RAbuseEmail:  info@volumedrive.com
RAbuseRef:    http://whois.arin.net/rest/poc/VOLUM-ARIN
RNOCHandle: VOLUM-ARIN
RNOCName:   VolumeDrive
RNOCPhone:  +1-862-266-1083
RNOCEmail:  info@volumedrive.com
RNOCRef:    http://whois.arin.net/rest/poc/VOLUM-ARIN
RTechHandle: VOLUM1-ARIN
RTechName:   VolumeDrive POC
RTechPhone:  +1-862-266-1083
RTechEmail:  info@volumedrive.com
RTechRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
```

inetnum: 188.132.241.0 - 188.132.241.255

```
netname:        Mars-Customer192
descr:          Mars-Customer192
country:        TR
org:            ORG-MGDS1-RIPE
admin-c:        MN4961-RIPE
tech-c:         MN4961-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-MARSNET
organisation:   ORG-MGDS1-RIPE
org-name:       Mars Global Datacenter Services LLC
org-type:       OTHER
address:        Pobrezni 118, Prague, Czech Republic Turkey
mnt-ref:        MNT-MARSNET
mnt-by:         MNT-MARSNET
person:         Mars Noc
address:        Nadiama St. No:28 Turkey
mnt-by:         MNT-MARSNET
phone:          +90 213 437 87 87
nic-hdl:        MN4961-RIPE
route:          188.132.241.0/24
descr:          MarsGlobal1-Net1
origin:         AS42910
mnt-by:         MNT-MARSNET
```

inetnum: 190.218/16

```
status:      allocated
aut-num:     N/A
owner:       Cable Onda
ownerid:     PA-CAON1-LACNIC
```

```
responsible: Climaco Manuel Paz
address:     Ave. 12 de Octubre, Pueblo Nuevo, Edif. Cable Onda, 0593,
address:     55-0593 - Panama - PA
country:     PA
phone:       +507 390 3485 []
owner-c:     CAO
tech-c:      CAO
abuse-c:     CAO
inetrev:     190.218/16
nserver:     NS3.CABLEONDA.NET
nsstat:      20130412 AA
nslastaa:    20130412
nserver:     NS2.CABLEONDA.NET  [lame - not published]
nsstat:      20130412 NOT SYNC ZONE
nslastaa:    20120321
nserver:     NS1.CABLEONDA.NET
nsstat:      20130412 AA
nslastaa:    20130412
created:     20081229
changed:     20081229
nic-hdl:     CAO
person:      Cable Onda Panama
e-mail:      ipadmin@CABLEONDA.NET
address:     Edificio Cable Onda, Pueblo Nuevo, 0, 0
address:     0831-0059 - Panama - PA
country:     PA
phone:       +507  3907616 []
created:     20021009
changed:     20071107
```

inetnum: 190.218/16

```
status:      allocated
aut-num:     N/A
owner:       Cable Onda
ownerid:     PA-CAON1-LACNIC
responsible: Climaco Manuel Paz
address:     Ave. 12 de Octubre, Pueblo Nuevo, Edif. Cable Onda, 0593,
address:     55-0593 - Panama - PA
country:     PA
phone:       +507 390 3485 []
owner-c:     CAO
tech-c:      CAO
abuse-c:     CAO
inetrev:     190.218/16
nserver:     NS3.CABLEONDA.NET
nsstat:      20130412 AA
nslastaa:    20130412
nserver:     NS2.CABLEONDA.NET  [lame - not published]
nsstat:      20130412 NOT SYNC ZONE
nslastaa:    20120321
nserver:     NS1.CABLEONDA.NET
nsstat:      20130412 AA
nslastaa:    20130412
created:     20081229
changed:     20081229
nic-hdl:     CAO
person:      Cable Onda Panama
e-mail:      ipadmin@CABLEONDA.NET
address:     Edificio Cable Onda, Pueblo Nuevo, 0, 0
address:     0831-0059 - Panama - PA
country:     PA
```

```
phone:       +507  3907616 []
created:     20021009
changed:     20071107

inetnum:     190.219/16
status:      allocated
aut-num:     N/A
owner:       Cable Onda
ownerid:     PA-CAON1-LACNIC
responsible: Climaco Manuel Paz
address:     Ave. 12 de Octubre, Pueblo Nuevo, Edif. Cable Onda, 0593,
address:     55-0593 - Panama - PA
country:     PA
phone:       +507 390 3485 []
owner-c:     CAO
tech-c:      CAO
abuse-c:     CAO
inetrev:     190.219/16
nserver:     NS3.CABLEONDA.NET
nsstat:      20130413 AA
nslastaa:    20130413
nserver:     NS1.CABLEONDA.NET
nsstat:      20130413 AA
nslastaa:    20130413
nserver:     NS2.CABLEONDA.NET  [lame - not published]
nsstat:      20130413 NOT SYNC ZONE
nslastaa:    20120402
created:     20100618
changed:     20100618
nic-hdl:     CAO
person:      Cable Onda Panama
e-mail:      ipadmin@CABLEONDA.NET
address:     Edificio Cable Onda, Pueblo Nuevo, 0, 0
address:     0831-0059 - Panama - PA
country:     PA
phone:       +507  3907616 []
created:     20021009
changed:     20071107

inetnum:     190.242.64/21
status:      reallocated
owner:       Columbus Networks Panama
ownerid:     PA-DEST-LACNIC
responsible: Jos\E9 Hern\E1ndez
address:     Plaza Obarrio, -, piso 3, oficina 303
address:     0823-0341 - Panama -
country:     PA
phone:       +507  2060100 []
owner-c:     FAA7
tech-c:      FAA7
abuse-c:     DES3
created:     20100528
changed:     20110407
inetnum-up:  190.242/16
nic-hdl:     DES3
person:      Denis Staff
e-mail:      dstaff@COLUMBUS-NETWORKS.COM.PA
address:     Edificio PH St Georges Bank Calle, 50, Piso 9
address:     00000 - Panama -
country:     PA
phone:       +507  2060100 []
```

```
created:     20090213
changed:     20090219
nic-hdl:     FAA7
person:      Fabio Anino
e-mail:      fanino@COLUMBUS-NETWORKS.COM.PA
address:     Plaza Obarrio, ,
address:      - Panama - PA
country:     PA
phone:       +507  66171487 []
created:     20110324
changed:     20120928
```

NetRange: 199.180.112.0 - 199.180.119.255

```
CIDR:           199.180.112.0/21
OriginAS:       AS46664
NetName:        VOLUM-ARIN
NetHandle:      NET-199-180-112-0-1
Parent:         NET-199-0-0-0-0
NetType:        Direct Allocation
RegDate:        2012-04-11
Updated:        2012-04-11
Ref:            http://whois.arin.net/rest/net/NET-199-180-112-0-1
OrgName:        VolumeDrive
OrgId:          VOLUM-2
Address:        1143 Northern Blvd
City:           Clarks Summit
StateProv:      PA
PostalCode:     18411
Country:        US
RegDate:        2008-08-26
Updated:        2011-09-24
Ref:            http://whois.arin.net/rest/org/VOLUM-2
OrgAbuseHandle: VOLUM1-ARIN
OrgAbuseName:   VolumeDrive POC
OrgAbusePhone:  +1-862-266-1083
OrgAbuseEmail:  info@volumedrive.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
OrgTechHandle: VOLUM1-ARIN
OrgTechName:   VolumeDrive POC
OrgTechPhone:  +1-862-266-1083
OrgTechEmail:  info@volumedrive.com
OrgTechRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
NetRange:       199.180.116.0 - 199.180.116.255
CIDR:           199.180.116.0/24
OriginAS:       AS46664
NetName:        VOLUM-ARIN
NetHandle:      NET-199-180-116-0-1
Parent:         NET-199-180-112-0-1
NetType:        Reallocated
RegDate:        2012-05-18
Updated:        2012-05-18
Ref:            http://whois.arin.net/rest/net/NET-199-180-116-0-1
OrgName:        UPVPS Hosting
OrgId:          UH-8
Address:        8220 Goldie
City:           Commerce Township
StateProv:      MI
PostalCode:     48382
Country:        US
RegDate:        2012-05-18
Updated:        2012-05-18
```

```
Ref:            http://whois.arin.net/rest/org/UH-8
OrgAbuseHandle: LUSKI-ARIN
OrgAbuseName:   Luski, Fred
OrgAbusePhone:  +1-862-266-1083
OrgAbuseEmail:  fredlky677@gmail.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/LUSKI-ARIN
OrgTechHandle: LUSKI-ARIN
OrgTechName:   Luski, Fred
OrgTechPhone:  +1-862-266-1083
OrgTechEmail:  fredlky677@gmail.com
OrgTechRef:    http://whois.arin.net/rest/poc/LUSKI-ARIN
```

NetRange: 199.180.112.0 - 199.180.119.255

```
CIDR:           199.180.112.0/21
OriginAS:       AS46664
NetName:        VOLUM-ARIN
NetHandle:      NET-199-180-112-0-1
Parent:         NET-199-0-0-0-0
NetType:        Direct Allocation
RegDate:        2012-04-11
Updated:        2012-04-11
Ref:            http://whois.arin.net/rest/net/NET-199-180-112-0-1
OrgName:        VolumeDrive
OrgId:          VOLUM-2
Address:        1143 Northern Blvd
City:           Clarks Summit
StateProv:      PA
PostalCode:     18411
Country:        US
RegDate:        2008-08-26
Updated:        2011-09-24
Ref:            http://whois.arin.net/rest/org/VOLUM-2
OrgTechHandle: VOLUM1-ARIN
OrgTechName:   VolumeDrive POC
OrgTechPhone:  +1-862-266-1083
OrgTechEmail:  info@volumedrive.com
OrgTechRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
OrgAbuseHandle: VOLUM1-ARIN
OrgAbuseName:   VolumeDrive POC
OrgAbusePhone:  +1-862-266-1083
OrgAbuseEmail:  info@volumedrive.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
NetRange:       199.180.117.0 - 199.180.117.255
CIDR:           199.180.117.0/24
OriginAS:       AS46664
NetName:        VOLUM-ARIN
NetHandle:      NET-199-180-117-0-1
Parent:         NET-199-180-112-0-1
NetType:        Reallocated
RegDate:        2012-05-18
Updated:        2012-05-18
Ref:            http://whois.arin.net/rest/net/NET-199-180-117-0-1
OrgName:        UPVPS Hosting
OrgId:          UH-9
Address:        8220 Goldie
City:           Commerce Township
StateProv:      MI
PostalCode:     48382
Country:        US
RegDate:        2012-05-18
Updated:        2012-05-18
```

```
Ref:            http://whois.arin.net/rest/org/UH-9
OrgAbuseHandle: LUSKI1-ARIN
OrgAbuseName:   Luski, Fred
OrgAbusePhone:  +1-862-266-1083
OrgAbuseEmail:  fredlky677@gmail.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/LUSKI1-ARIN
OrgTechHandle: LUSKI1-ARIN
OrgTechName:   Luski, Fred
OrgTechPhone:  +1-862-266-1083
OrgTechEmail:  fredlky677@gmail.com
OrgTechRef:    http://whois.arin.net/rest/poc/LUSKI1-ARIN

NetRange:       199.19.104.0 - 199.19.111.255
CIDR:           199.19.104.0/21
OriginAS:       AS46664
NetName:        VOLUMEDRIVE
NetHandle:      NET-199-19-104-0-1
Parent:         NET-199-0-0-0-0
NetType:        Direct Allocation
RegDate:        2011-10-07
Updated:        2012-03-02
Ref:            http://whois.arin.net/rest/net/NET-199-19-104-0-1
OrgName:        VolumeDrive
OrgId:          VOLUM-2
Address:        1143 Northern Blvd
City:           Clarks Summit
StateProv:      PA
PostalCode:     18411
Country:        US
RegDate:        2008-08-26
Updated:        2011-09-24
Ref:            http://whois.arin.net/rest/org/VOLUM-2
OrgAbuseHandle: VOLUM1-ARIN
OrgAbuseName:   VolumeDrive POC
OrgAbusePhone:  +1-862-266-1083
OrgAbuseEmail:  info@volumedrive.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN
OrgTechHandle: VOLUM1-ARIN
OrgTechName:   VolumeDrive POC
OrgTechPhone:  +1-862-266-1083
OrgTechEmail:  info@volumedrive.com
OrgTechRef:    http://whois.arin.net/rest/poc/VOLUM1-ARIN

inetnum:     200.46.0/17
status:      allocated
aut-num:     N/A
owner:       Net2Net Corp.
ownerid:     PA-SINF-LACNIC
responsible: IP Admin
address:     Plaza Bal Harbour, 1,
address:     55-0779 - Panama - PA
country:     PA
phone:       +507  2063000 []
owner-c:     NEA3
tech-c:      NEA3
abuse-c:     NEA3
inetrev:     200.46.8/22
nserver:     NS.PSINETPA.NET
nsstat:      20130413 AA
nslastaa:    20130413
nserver:     NS2.PSINETPA.NET
```

```
nsstat:      20130413 TIMEOUT
nslastaa:    20130407
created:     19981221
changed:     20020502
nic-hdl:     NEA3
person:      Net2Net Admin
e-mail:      ipadmin@NET2NET.COM.PA
address:     Plaza Bal Harbour Paitilla, 1,
address:     55-0779 - Panama - PA
country:     PA
phone:       +507  206-3000 [ATM]
created:     20030414
changed:     20091028
```

inetnum: 201.218.224/19

```
status:      allocated
aut-num:     N/A
owner:       Net2Net Corp.
ownerid:     PA-SINF-LACNIC
responsible: IP Admin
address:     Plaza Bal Harbour, 1,
address:     55-0779 - Panama - PA
country:     PA
phone:       +507  2063000 []
owner-c:     NEA3
tech-c:      NEA3
abuse-c:     NEA3
inetrev:     201.218.255/24
nserver:     NS1.TCARRIER.NET
nsstat:      20130412 AA
nslastaa:    20130412
nserver:     NS2.TCARRIER.NET
nsstat:      20130412 AA
nslastaa:    20130412
created:     20070509
changed:     20070509
nic-hdl:     NEA3
person:      Net2Net Admin
e-mail:      ipadmin@NET2NET.COM.PA
address:     Plaza Bal Harbour Paitilla, 1,
address:     55-0779 - Panama - PA
country:     PA
phone:       +507  206-3000 [ATM]
created:     20030414
changed:     20091028
inetnum:        85.25.129.0 - 85.25.153.255
descr:          BSB-SERVICE Dedicated Server Hosting
netname:        BSB-SERVICE-1
country:        DE
org:            ORG-BSBS1-RIPE
admin-c:        NPA10-RIPE
tech-c:         NPA10-RIPE
status:         ASSIGNED PA
mnt-by:         BSB-SERVICE-MNT
organisation:   ORG-BSBS1-RIPE
org-name:       B S B - Service GmbH
org-type:       OTHER
descr:          Internet-Hoster
address:        Daimlerstr.9-11
address:        50354 Huerth
address:        Germany
```

```
phone:          +49 2233 612-0
fax-no:         +49 2233 612-144
admin-c:        NPA10-RIPE
tech-c:         NPA10-RIPE
mnt-ref:        INTERGENIA-MNT
mnt-by:         INTERGENIA-MNT
role:           NMC PlusServer AG
address:        PlusServer AG
address:        Daimlerstr. 9-11
address:        50354 Huerth
phone:          +49 1801 119991
fax-no:         +49 2233 612-53500
abuse-mailbox:  abuse@plusserver.de
admin-c:        JBPS-RIPE
tech-c:         CDPS-RIPE
tech-c:         ADPS-RIPE
nic-hdl:        NPA10-RIPE
mnt-by:         INTERGENIA-MNT
route:          85.25.0.0/16
descr:          PlusServer AG
origin:         AS8972
mnt-by:         INTERGENIA-MNT

inetnum:        85.25.246.0 - 85.25.246.255
descr:          BSB-SERVICE Dedicated Server Hosting
netname:        BSB-SERVICE-1
country:        DE
org:            ORG-BSBS1-RIPE
admin-c:        NPA10-RIPE
tech-c:         NPA10-RIPE
status:         ASSIGNED PA
mnt-by:         BSB-SERVICE-MNT
organisation:   ORG-BSBS1-RIPE
org-name:       B S B - Service GmbH
org-type:       OTHER
descr:          Internet-Hoster
address:        Daimlerstr.9-11
address:        50354 Huerth
address:        Germany
phone:          +49 2233 612-0
fax-no:         +49 2233 612-144
admin-c:        NPA10-RIPE
tech-c:         NPA10-RIPE
mnt-ref:        INTERGENIA-MNT
mnt-by:         INTERGENIA-MNT
role:           NMC PlusServer AG
address:        PlusServer AG
address:        Daimlerstr. 9-11
address:        50354 Huerth
phone:          +49 1801 119991
fax-no:         +49 2233 612-53500
abuse-mailbox:  abuse@plusserver.de
admin-c:        JBPS-RIPE
tech-c:         CDPS-RIPE
tech-c:         ADPS-RIPE
nic-hdl:        NPA10-RIPE
mnt-by:         INTERGENIA-MNT
route:          85.25.0.0/16
descr:          PlusServer AG
origin:         AS8972
mnt-by:         INTERGENIA-MNT
```

```
inetnum:        87.139.128.0 - 87.139.255.255
netname:        DTAG-STATIC06
descr:          Deutsche Telekom AG
           T-DSL Business
           static dial-up
country:        DE
admin-c:        DTIP
tech-c:         DTST
status:         ASSIGNED PA
           * Abuse Contact:              *
           * http://www.t-com.de/ip-abuse   *
           * in case of Spam, Hack Attacks, *
           * Illegal Activity, Violation,   *
           * Scans, Probes, etc.            *
           **********************************
mnt-by:         DTAG-NIC
person:         DTAG Global IP-Addressing
address:        Deutsche Telekom AG
address:        D-90492 Nuernberg
address:        Germany
phone:          +49 180 5334332
fax-no:         +49 6151 6809399
nic-hdl:        DTIP
mnt-by:         DTAG-NIC
person:         Security Team
address:        Deutsche Telekom AG
address:        Germany
phone:          +49 180 5334332
fax-no:         +49 6151 6809399
nic-hdl:        DTST
mnt-by:         DTAG-NIC
route:          87.128.0.0/11
descr:          Deutsche Telekom AG, Internet service provider
origin:         AS3320
member-of:        AS3320:RS-PA-TELEKOM
mnt-by:         DTAG-RR
```

Your Global e-Security Partner

www.glesec.com
info@glesec.com

United States

Worldwide Corporate HQ
Address. 66 Witherspoon Street
Princeton, NJ 08542
Tel. 609.651.4246

Panama

Central America HQ
Address. Edificio Century Tower
El Dorado, 12th Floor
Panama City, Panama
Tel. +507.836.5355

Argentina

South America HQ
+54.11.5917.6120

Brazil

+55.11.3711.5699

Chile

+56.2938.1496

Peru

+51.1708.7197

Mexico

+52.55.5018.116