www.glesec.com

GLESEC

Your Global e-security Partner

MONTHLY SECURITY REPORT

PREPARED FOR: METROBANK

FEBRUARY 2013

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.

Index

1. About this report

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 FEBRUARY 1, 2013 to FEBRUARY 28, 2013

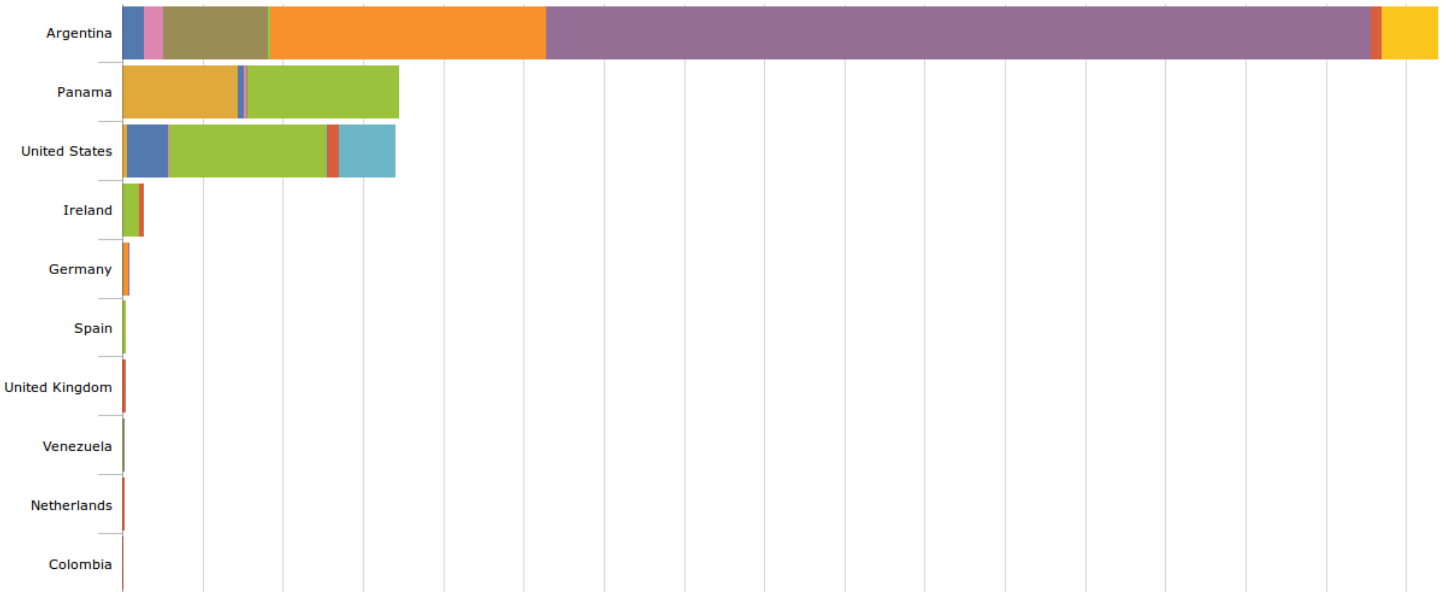
GLESEC would like to state for the record that a Security Assessment was performed by Carlos Tori (GA&C) this month which adversely affected this period's data. The traffic generated was immediately noticed by the GLESEC Incident Response team, but it was allowed to continue to gain the maximum benefit of the full Security Assessment. In a real world situation GLESEC would have immediately blacklisted the attacking IP and reported the offending IP to METROBANK in order for METROBANK to take the same action at carrier and/or router level.

Based on the information gathered from the DefensePro during this period **6,177** attacks on METROBANK, **274** of which were considered critical were all stopped by the Radware DefensePro 508. During the previous period, 9,254 attacks on METROBANK, 101 of which were considered critical were all stopped by the Radware DefensePro 508. The overall quantity of attacks dropped compared to the previous period although critical attacks nearly tripled.

Critical Flood attacks were common and included the following: network flood IPv4 UDP, network flood IPv4 TCP-SYN, network flood IPv4 TCP-RST attacks. Threat agents were unsuccessful in utilizing blended multi-vector attacks in attempt to bypass protection mechanisms. Rate Limiting, Network Behavioral Analysis, DoS Protection and Signature (IPS) Protection assisted in mitigating these attack vectors.

Server Cracking and Anti Scanning Protection played a large part in defending servers by dropping the malicious traffic including: Brute Force Web, Brute Force DNS, and Web Scan, SIP-Scanner-SIPVicious, BO-Apache-HTTPD-log-Cookie attempts. GLESEC discovered attacks directed at well-known port numbers: 443 (https), 25 (smtp), 80 (http), 5060 (sip), 1713 (conferencetalk) ,8080 (http-alt) in order of frequency. High port numbers were also frequently probed this month, a not so common occurrence that was a product of the Security Assessment that took place. Port number information utilized is based on IANA Service Name and Transport Protocol Port Number Registry.

Scanning and reconnaissance were extremely prevalent this report period which utilized various methods in attempt to enumerate the METROBANK infrastructure/services such as: TCP Scan, TCP Scan (vertical), TCP Scan (horizontal), UDP Scan, UDP Scan (horizontal), UDP Scan (vertical), and Ping Sweeps were a regular occurrence and are geographically most prevalent from Argentina as depicted in the following graph:



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.

4. Recommendations

GLESEC recommends for METROBANK to review the following Critical Controls: 3, 4, 5, 6 in response to Brute Forcing (Cracking Protection) and Scanning (Anti Scanning) attempts viewed in this period. Specifically adding

a Vulnerability Management Service coupled with a METROBANK remediation policy would significantly decrease the attack surface, avoiding script-kiddies and automated attacks.

METROBANK is recommended to implement Critical Control 14 by way of a Security Information and Event Management (SIEM) solution. This would provide a method to analyze logs and events across the organization more efficiently. A SIEM would allow immediate insight into the health of the organization and threat landscape as a whole, in order to respond pro-actively to all types of events. If METROBANK already utilizes a SIEM, providing GLESEC access would significantly improve security analysis and incident response.

GLESEC also recommends METROBANK utilize the **Twenty Critical Security Controls for Effective Cyber Defense** 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 SANS and GLESEC has included the links to the information below:

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs

- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response Capability
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

GLESEC offers many services and products that would assist in securing METROBANK to a greater degree. Some of our services are included in the section that follows. If interested in additional information about our offerings please contact info@glesec.com

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

GLESEC Services:

MSS: Managed Security Service (full outsourcing)

SSP: Security Support Program (systems management and support)

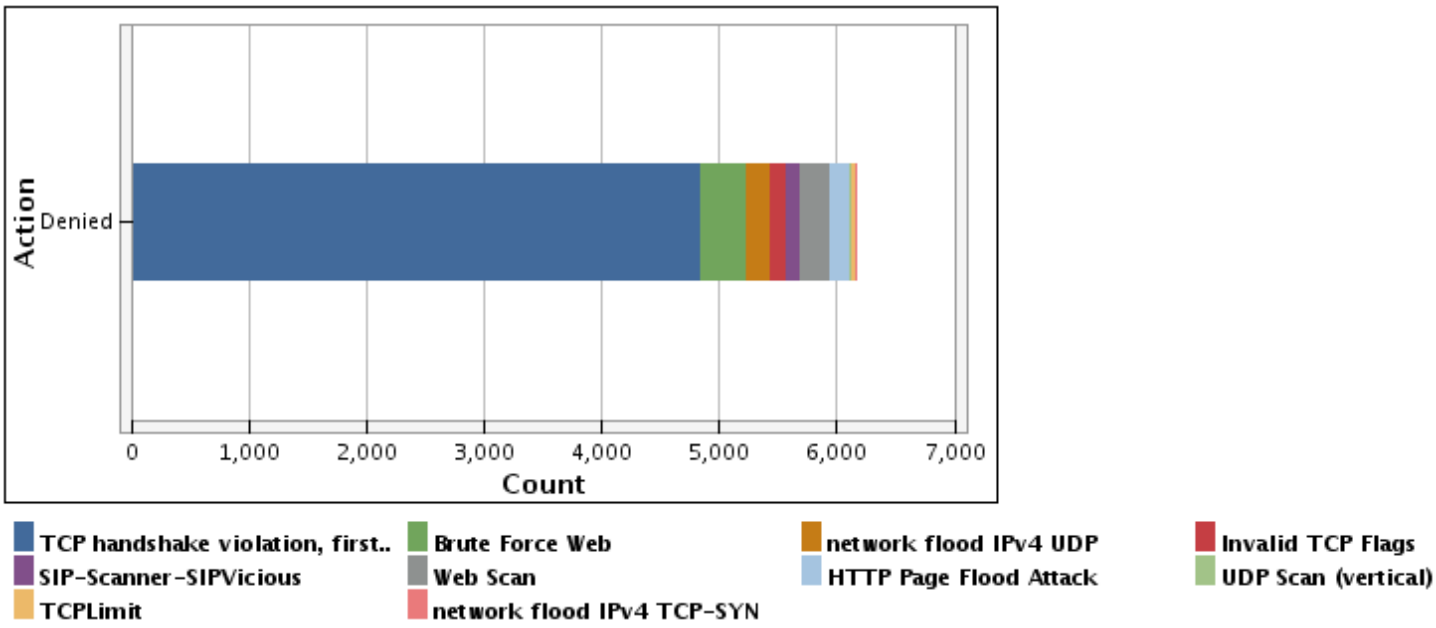
METROBANK Systems: Radware DefensePro 508

METROBANK Systems: Radware AppWall ODS1XL (Data Incomplete: Full report will be provided next month)

6. Detailed Security Report

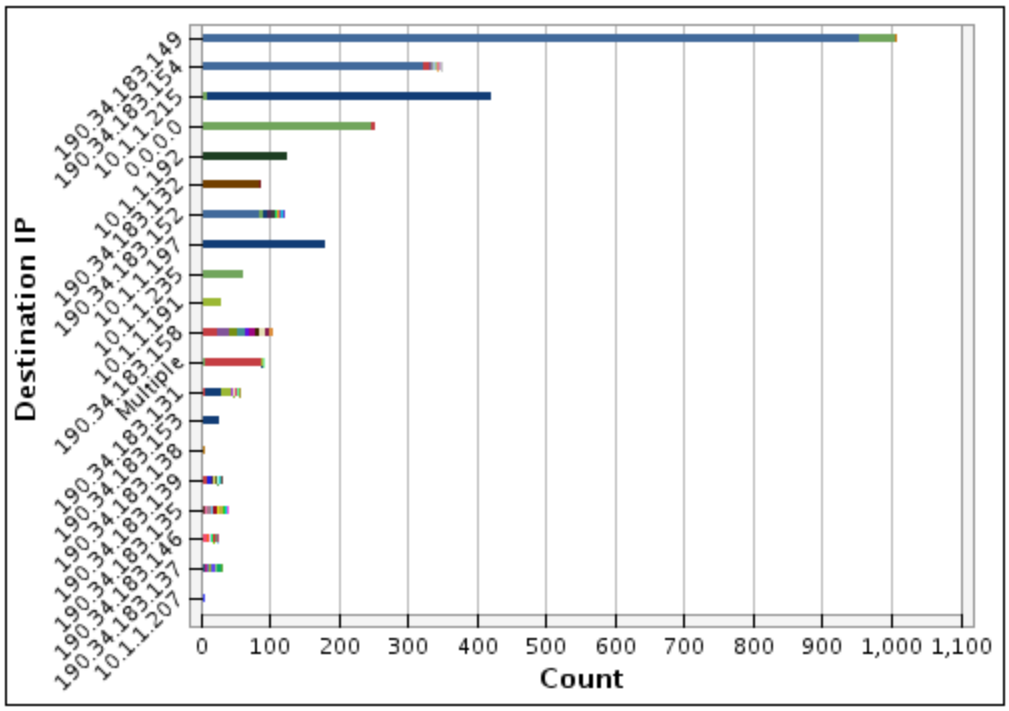
Graph: Attacks Allowed and Denied

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



Graph: Attacks by Destination and Port

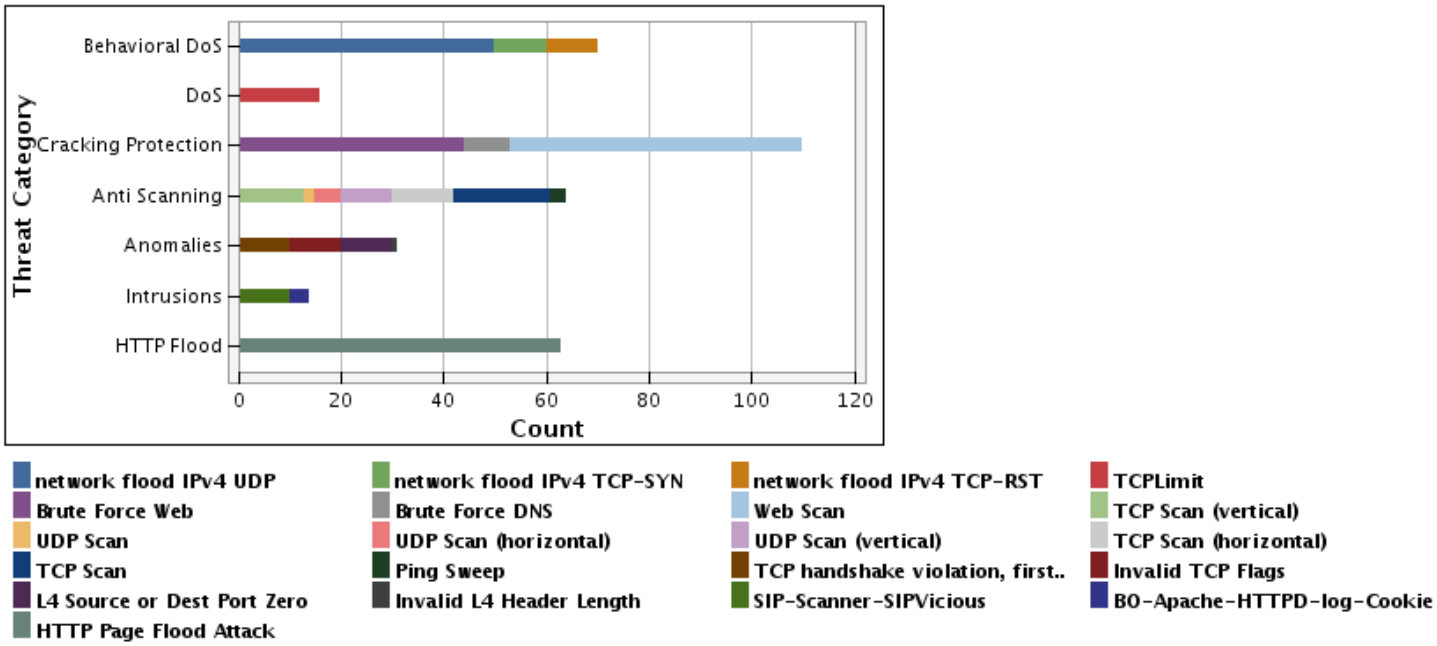
This report provides information on the total number of attacks that were attempted on which target device and port and for how many times, along with the attack name, network security rule.



443
0
25
Multiple
13063
11168
30890
46946
52594
12974
29912
28456
80
5060
4500
17596
2822
2032
1854
1713
3080
4064
3652
8080
16698
21390
44133
36496
20941
17718
17821
15060
32591
5080
4830
3196
4229
8184
1389
4362
8200
2070
1432
3756
2228
1113
1693
2067
1441
19737
24242
46111
40220
38426
41303
51436
34603
52558
12400
59955
50956
55692
52642
59600

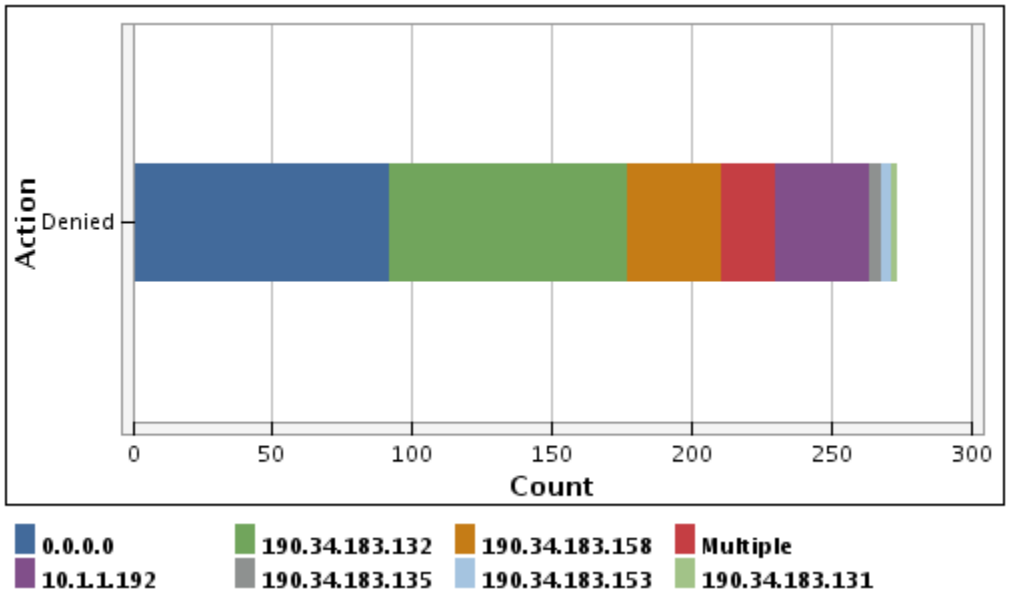
Graph: Attacks By Threat Category

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



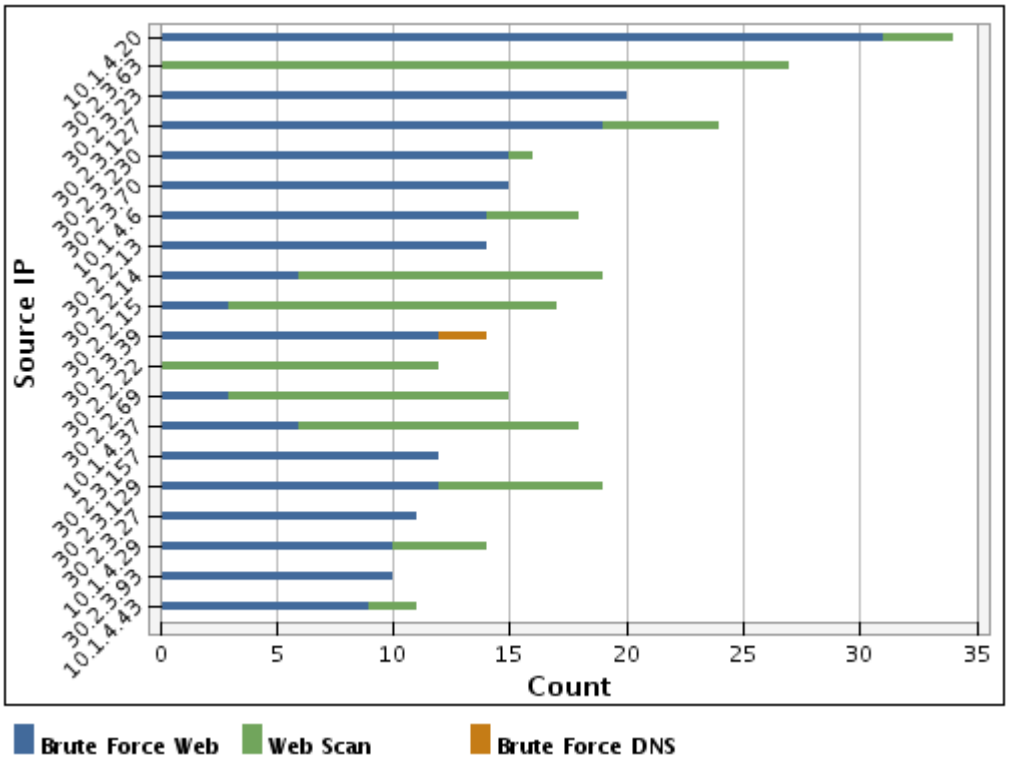
Graph: Critical Attacks

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.



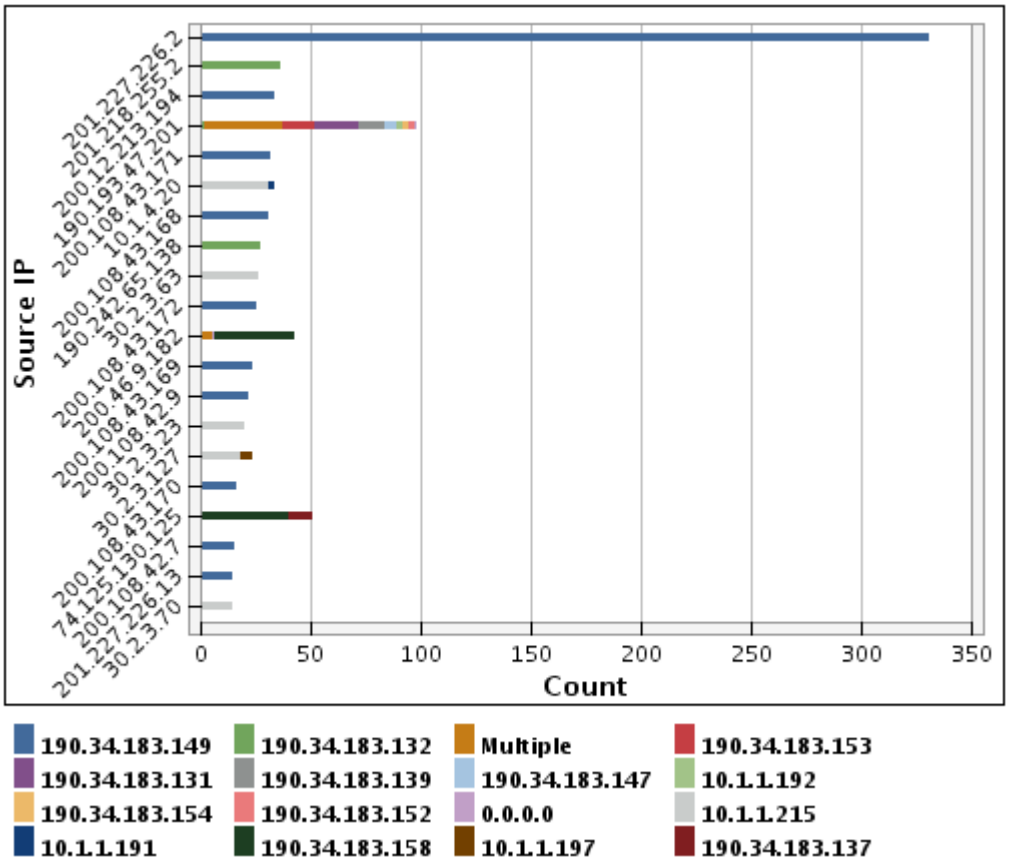
Graph: Internal Attacks by Sources

You can view information on the attacks, the internal source that was responsible for the attack, attack name, network security rule along with the total number of times the attack was launched.



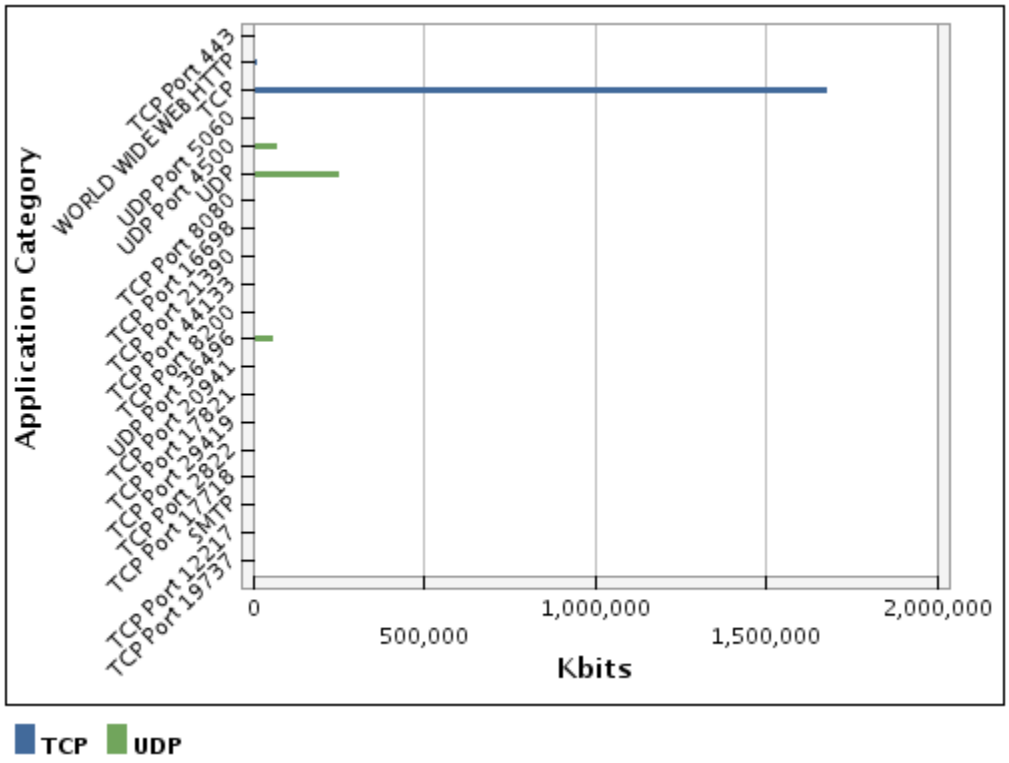
Graph: Top Attack Sources Blocked

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.



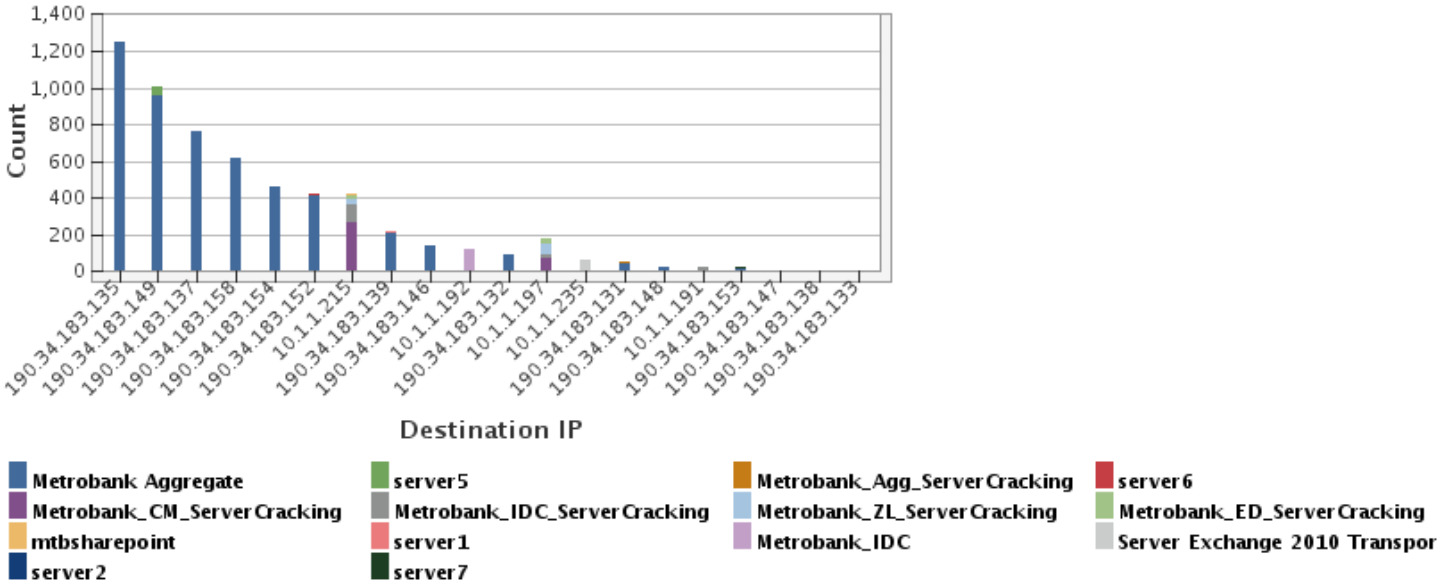
Graph: Top Attacked Applications

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).



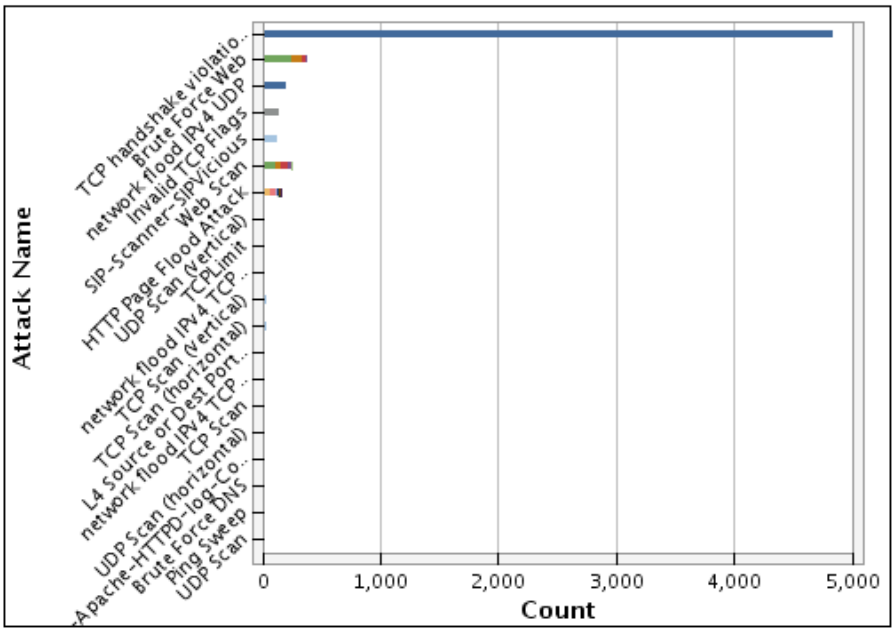
Graph: Top Attacked Destinations

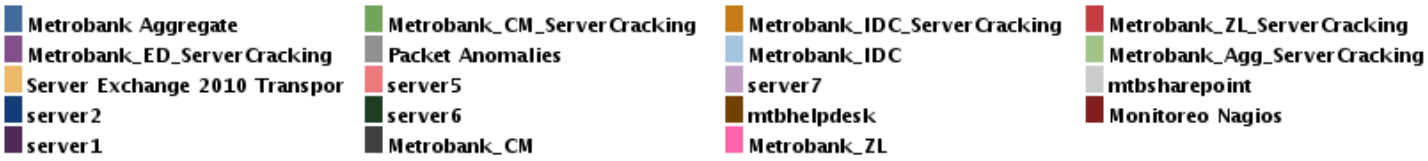
This report provides information on the system IPs, which were the destination of the attacks for most number of times along with the network security rule.



Graph: Top Attacks Blocked

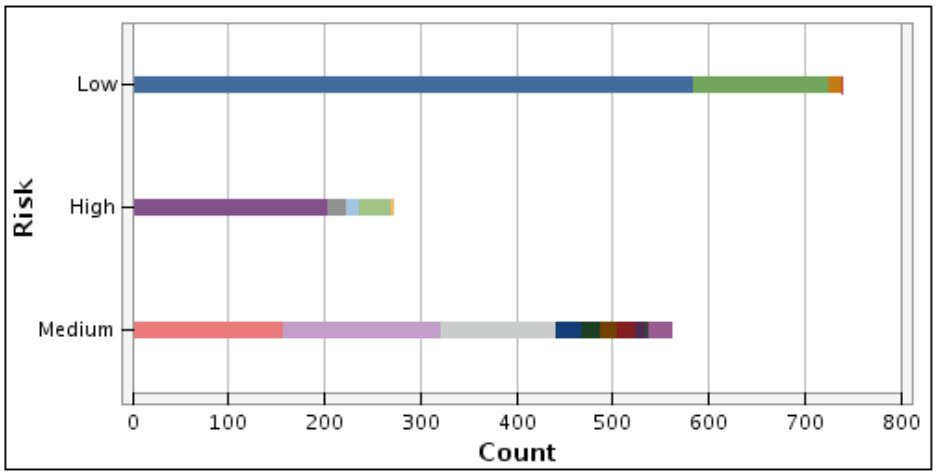
This report provides information on the Top Attacks Blocked, the attack name, network security rule and VLAN and the total number of attacks blocked with this combination.





Graph: Top Attacks Blocked By Risk

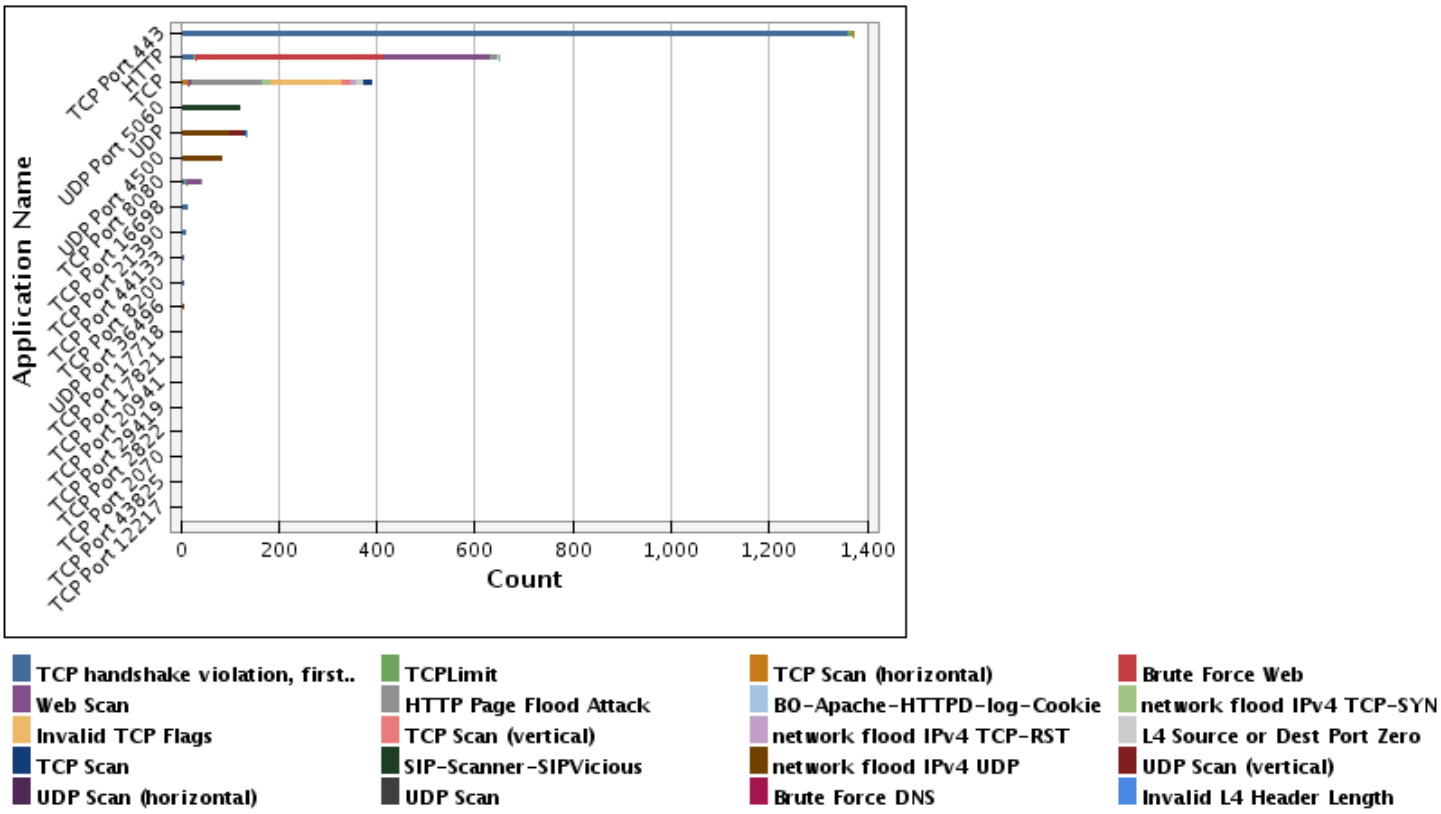
This report provides information on the attacks, which were blocked on DP IPS based on their risk. In this report the risk of the attack, attack name, source, destination, the destination port, network security rules are shown.



TCP handshake violation, first..
Invalid TCP Flags
L4 Source or Dest Port Zero
Invalid L4 Header Length
network flood IPv4 UDP
network flood IPv4 TCP-SYN
network flood IPv4 TCP-RST
SIP-Scanner-SIPVicious
BO-Apache-HTTPD-log-Cookie
HTTP Page Flood Attack
Brute Force Web
Web Scan
UDP Scan (vertical)
TCP Scan
TCP Scan (horizontal)
TCP Scan (vertical)
Brute Force DNS
UDP Scan (horizontal)
TCPLimit

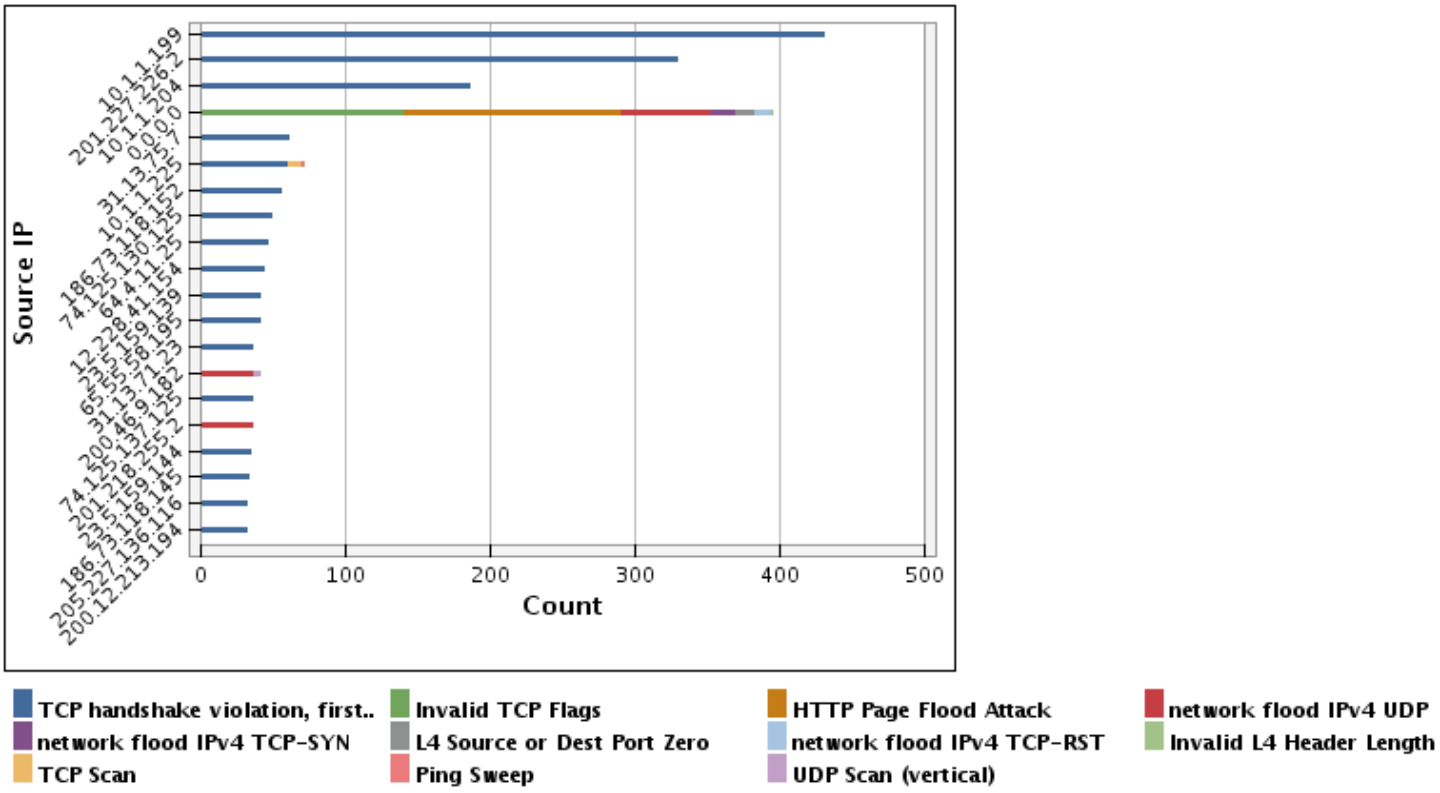
Graph: Top Attacks by Application

This report provides information on the total number of top attacks attempted on a device, the attack name, the protocol through which the attack was attempted, network security rule and VLAN.



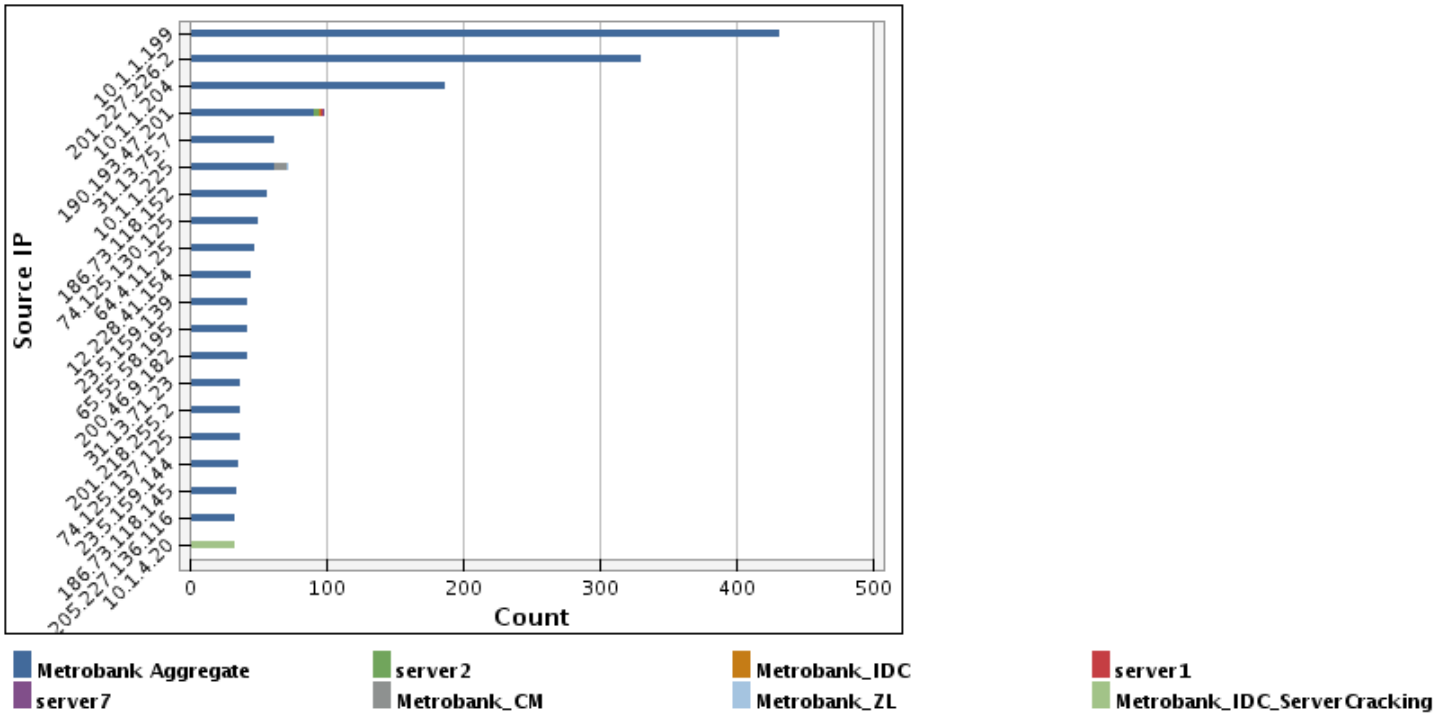
Graph: Top Attacks by Source

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.



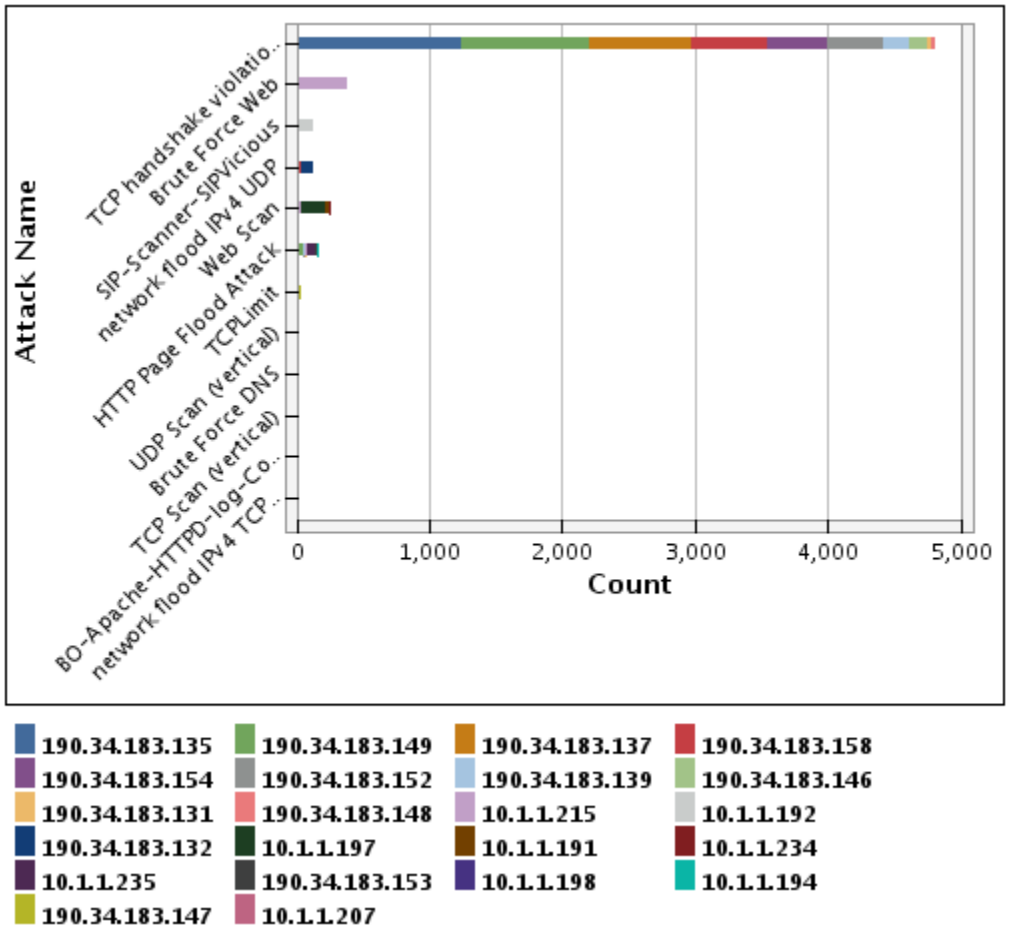
Graph: Top Denied Attackers

This report displays the IP addresses of the sources that were the top denied attack sources and the number of times an attempted attack was denied from each source along with the network security rule and VLAN . Note: This report does not show IP addresses which are either 'NULL' or '0.0.0.0' or 'multiple'.



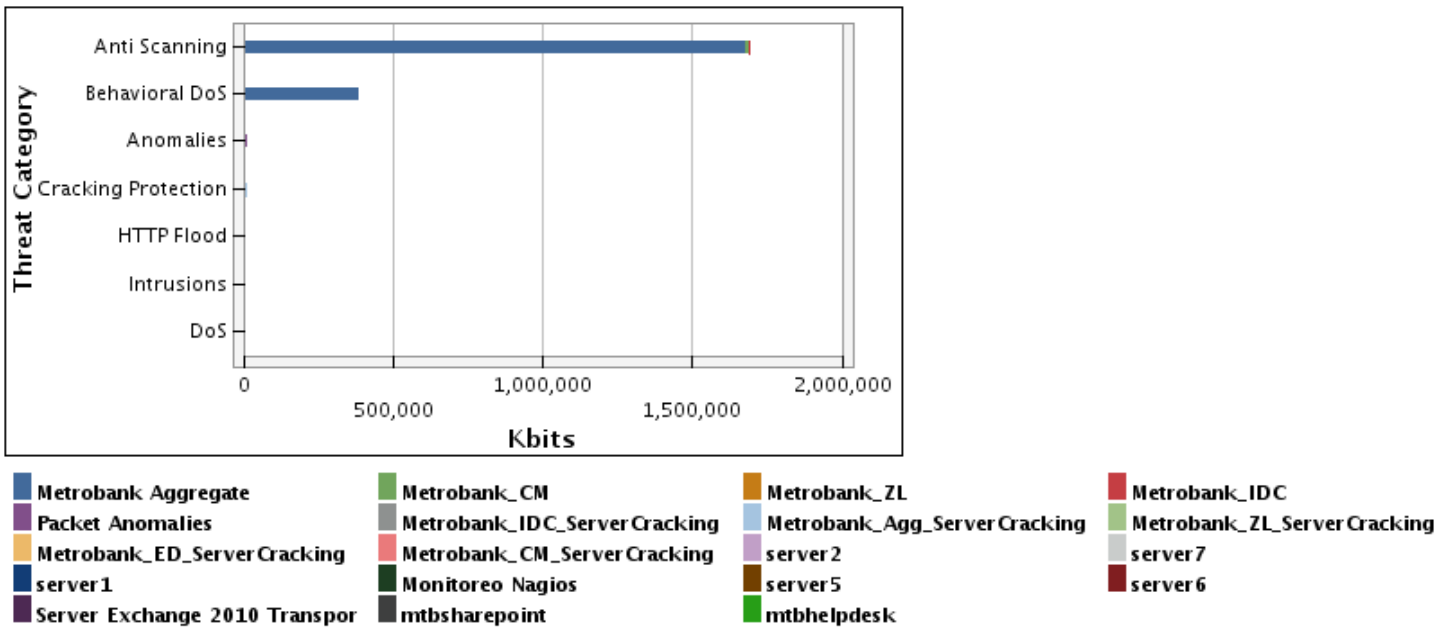
Graph: Top Destinations by Attack

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.



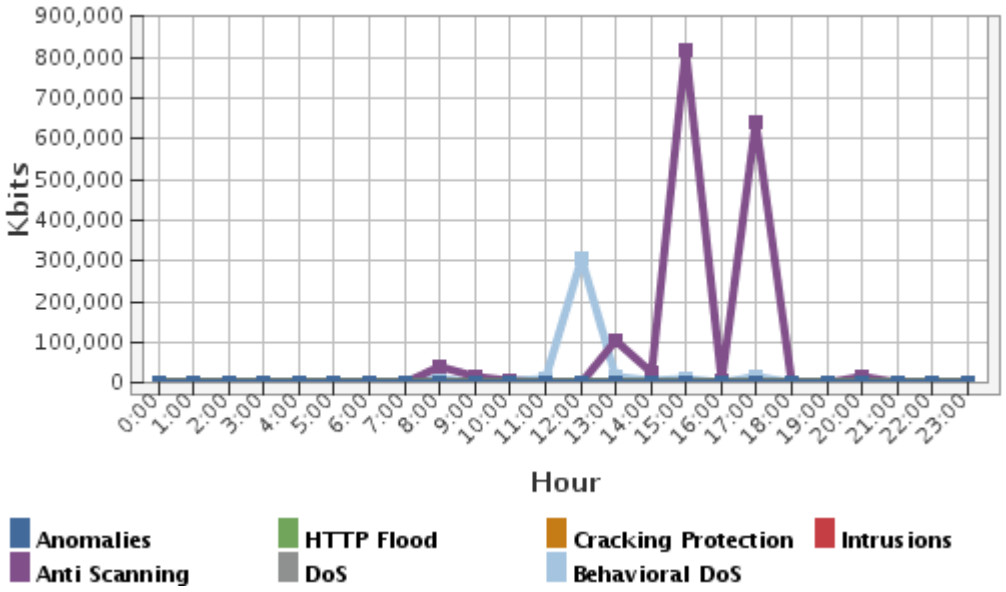
Graph: Attack Categories by Bandwidth

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.



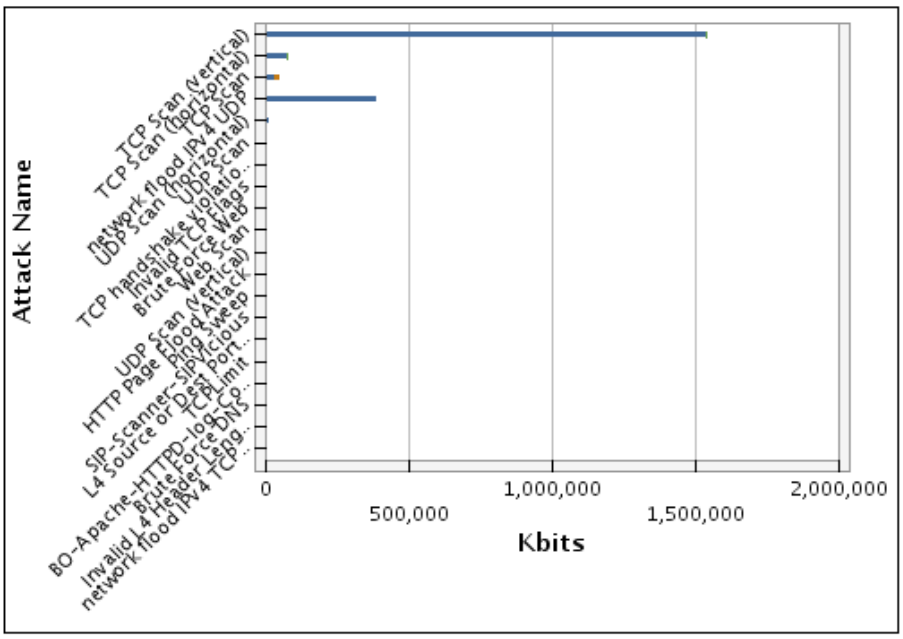
Graph: Bandwidth by Threat Category by Hour of Day

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.



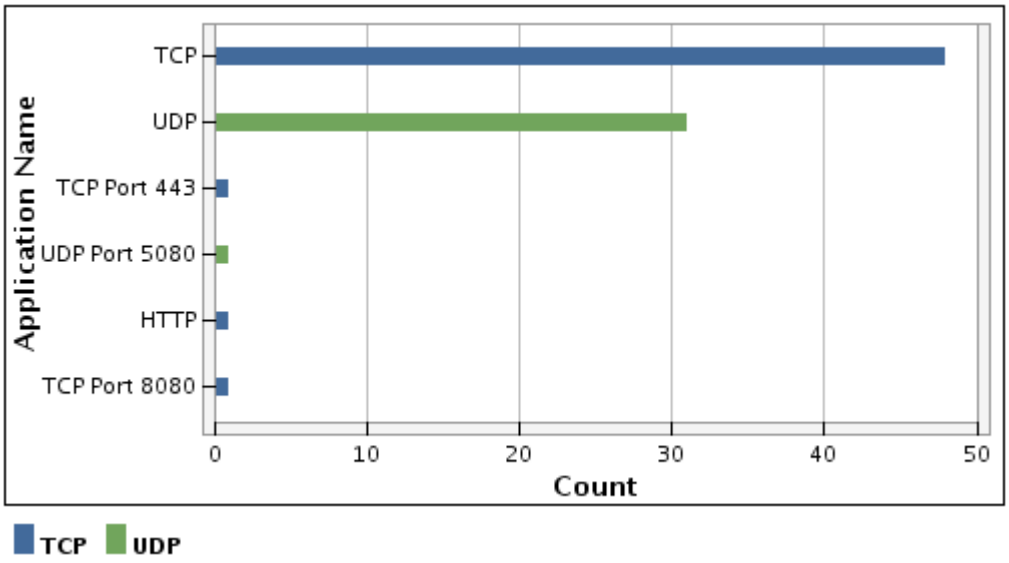
Graph: Top Attacks by Bandwidth

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.



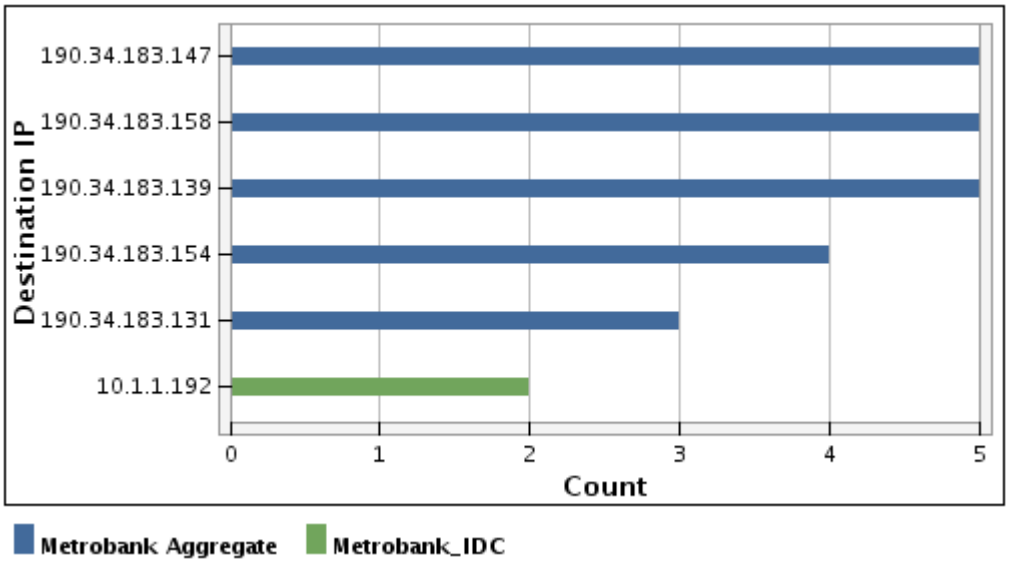
Graph: Top Probed Applications

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.



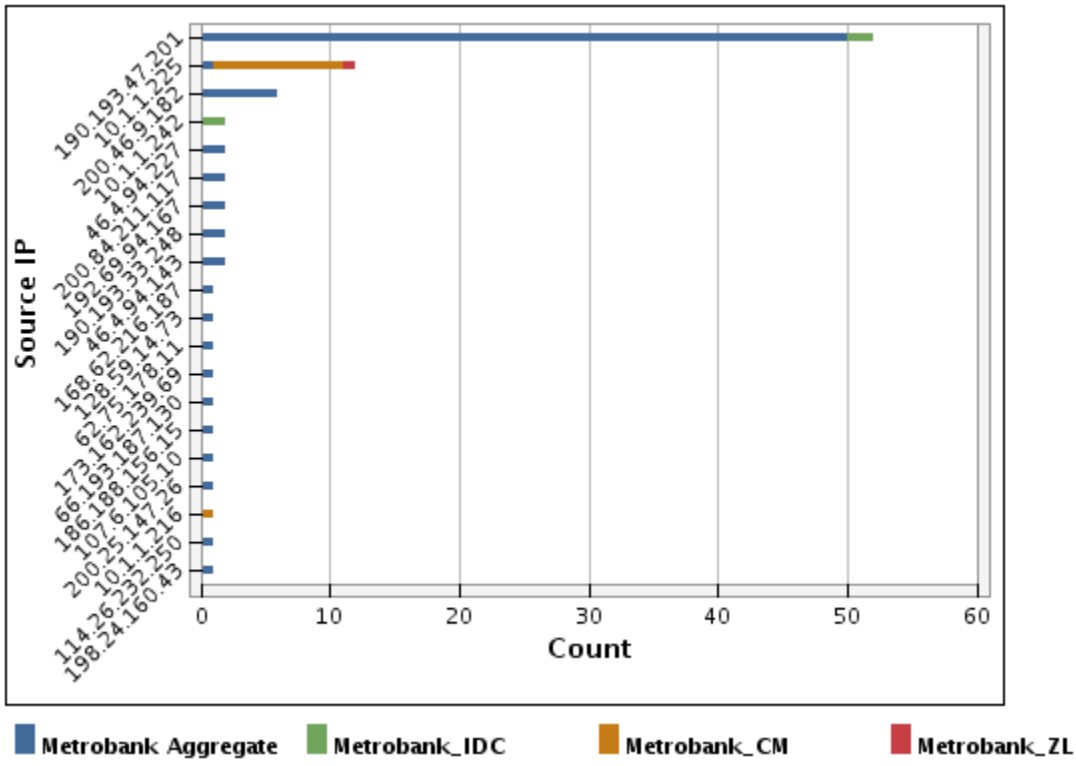
Graph: Top Probed IP Addresses

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.



NOTE: See Appendix 1 – Top Scanners (Source IP Addressed) (WHOIS Information)

7. Detailed Security Operations Systems Report

This section of the report represents the activities performed by GLESEC's Global Operations Center. These include:

a) Monitoring of system availability

METROBANK DefensePro Availability:

The DefensePro was considered up and available 99.969% of time of time during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	27d 23h 47m 40s	99.969%	99.969%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	27d 23h 47m 40s	99.969%	99.969%
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	0.027%	0.027%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 11m 0s	0.027%	0.027%
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	28d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.852% (99.852%)	0.024% (0.024%)	0.000% (0.000%)	0.124% (0.124%)	0.000%
Average	99.852% (99.852%)	0.024% (0.024%)	0.000% (0.000%)	0.124% (0.124%)	0.000%

b) Monitoring system performance

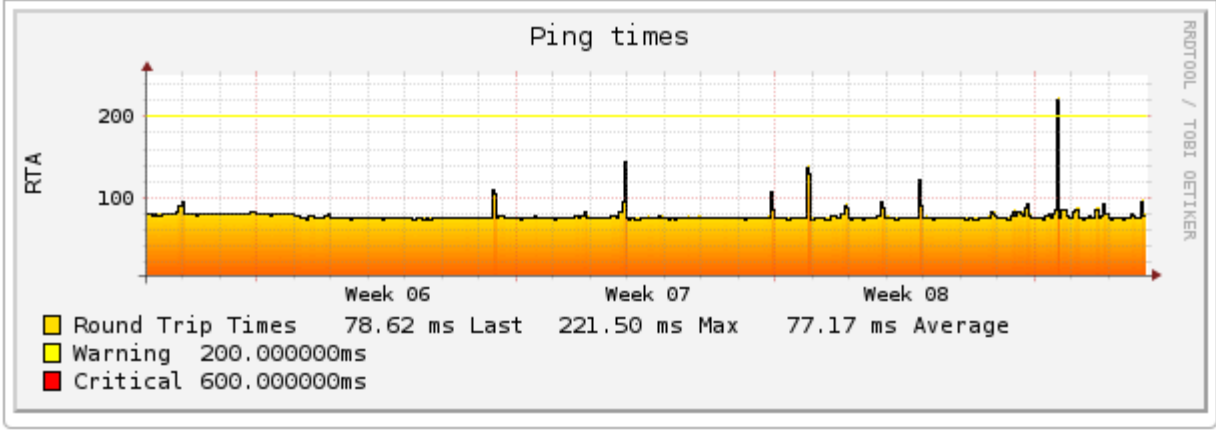
METROBANK DefensePro Ping Performance:

Round trip ping times averaged 77.17 ms from the GLESEC GOC to METROBANK with 0% average packet loss

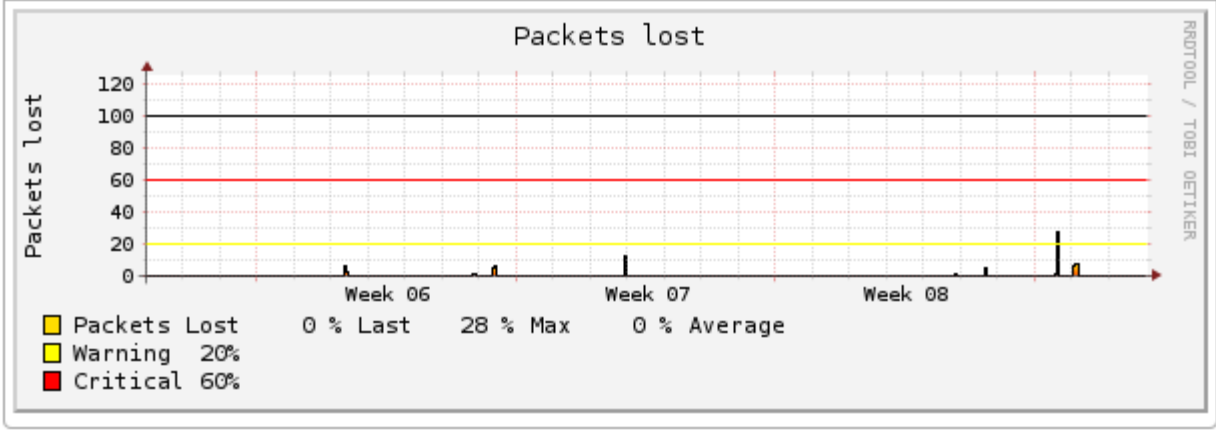
Host: MetroBank DefensePro 508 **Service:** PING

Custom time range 01.02.13 0:00 - 28.02.13 0:00

Datasource: Round Trip Times



Datasource: Packets Lost



METROBANK AppWall Availability: The AppWall was considered up and available 99.979 % of time of time during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	27d 23h 51m 30s	99.979%	99.979%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	27d 23h 51m 30s	99.979%	99.979%
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	0.021%	0.021%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 8m 30s	0.021%	0.021%
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	28d 0h 0m 0s	100.000%	100.000%

M

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.864% (99.864%)	0.025% (0.025%)	0.000% (0.000%)	0.111% (0.111%)	0.000%
Average	99.864% (99.864%)	0.025% (0.025%)	0.000% (0.000%)	0.111% (0.111%)	0.000%

ETR

OB

AN

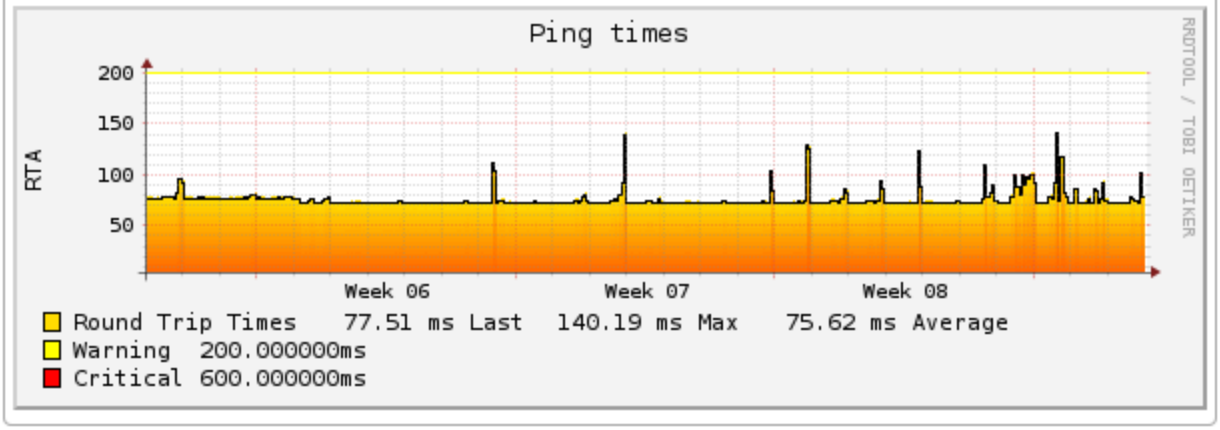
K AppWall Ping Performance:

Round trip ping times averaged 75.62 ms from the GLESEC GOC to METROBANK with 0% average packet loss

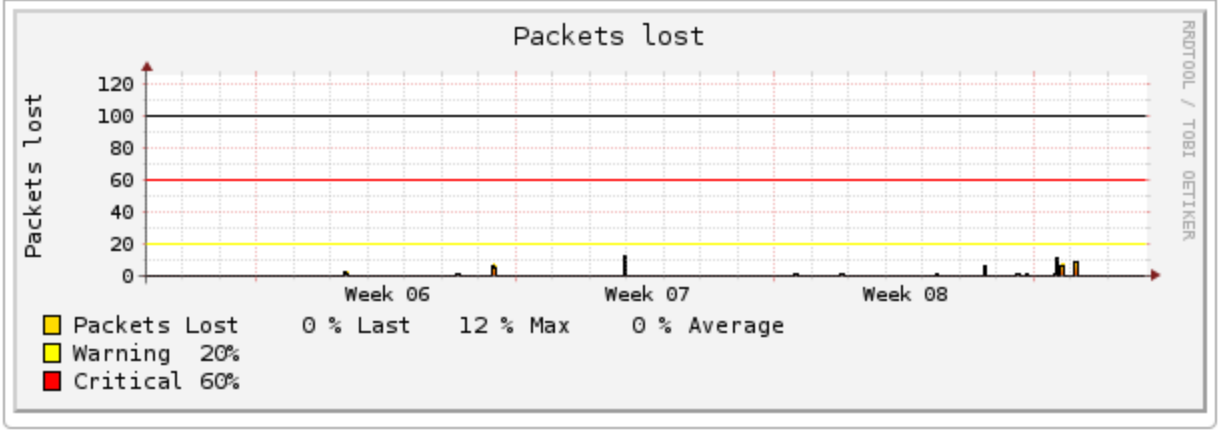
Host: MetroBank AppWall **Service:** PING

Custom time range 01.02.13 0:00 - 28.02.13 0:00

Datasource: Round Trip Times



Datasource: Packets Lost



c) Change management procedures

METROBANK Change Management: N/A

d) Incident Response procedures

METROBANK Incident Report: N/A

8. Appendix 1 - Top Scanners (Source IP Addressed) WHOIS Information

This section provides additional WHOIS detail for the **Graph: Top Scanners (Source IP Addressed)**

NetRange: 107.6.64.0 - 107.6.127.255

CIDR: 107.6.64.0/18

OriginAS: AS29791

NetName: VOXEL-NET-10

NetHandle: NET-107-6-64-0-1

Parent: NET-107-0-0-0-0

NetType: Direct Allocation

Comment: Re-assignment data at whois.voxel.net:4321.

Comment: Abuse complaints to abuse@voxel.net.

RegDate: 2011-02-02

Updated: 2012-03-02

Ref: http://whois.arin.net/rest/net/NET-107-6-64-0-1

OrgName: Voxel Dot Net, Inc.

OrgId: VDN-1

Address: 29 Broadway

Address: 30th Floor

City: New York

StateProv: NY

PostalCode: 10006

Country: US

RegDate: 2000-05-06

Updated: 2011-08-11

Ref: http://whois.arin.net/rest/org/VDN-1

ReferralServer: rwhois://rwhois.voxel.net:4321

OrgTechHandle: VOXEL-ARIN

OrgTechName: Voxel NOC

OrgTechPhone: +1-212-812-4190

OrgTechEmail: noc@voxel.net

OrgTechRef: http://whois.arin.net/rest/poc/VOXEL-ARIN

OrgNOCHandle: VOXEL-ARIN

OrgNOCName: Voxel NOC

OrgNOCPhone: +1-212-812-4190

OrgNOCEmail: noc@voxel.net

OrgNOCRef: http://whois.arin.net/rest/poc/VOXEL-ARIN

OrgAbuseHandle: VAD4-ARIN

OrgAbuseName: Voxel Abuse Desk

OrgAbusePhone: +1-212-812-4195

OrgAbuseEmail: abuse@voxel.net

OrgAbuseRef: http://whois.arin.net/rest/poc/VAD4-ARIN

RTechHandle: VOXEL-ARIN

RTechName: Voxel NOC

RTechPhone: +1-212-812-4190

RTechEmail: noc@voxel.net

RTechRef: http://whois.arin.net/rest/poc/VOXEL-ARIN

RAbuseHandle: VAD4-ARIN

RAbuseName: Voxel Abuse Desk

RAbusePhone: +1-212-812-4195

RAbuseEmail: abuse@voxel.net

RAbuseRef: http://whois.arin.net/rest/poc/VAD4-ARIN

RNOCHandle: VOXEL-ARIN

RNOCName: Voxel NOC

RNOCPhone: +1-212-812-4190

RNOCEmail: noc@voxel.net

RNOCRef: http://whois.arin.net/rest/poc/VOXEL-ARIN

Found a referral to rwhois.voxel.net:4321.

autharea=107.6.104.0/22

xautharea=107.6.104.0/22

network:Class-Name:network

network:Auth-Area:107.6.104.0/22

network:ID:NET-50155.107.6.105.10

network:Network-Name:107.6.105.8/29

network:IP-Network:107.6.105.10

network:IP-Network-Block:107.6.105.10

network:Org-Name:Neustar (Quova)

network:Street-Address:401 Castrol Street

network:City:Mountain View

network:State:CA

network:Postal-Code:94041

network:Country-Code:US

network:Tech-Contact:MAINT-50155.107.6.105.10

network:Created:20120606010920000

network:Updated:20120920061309000

network:Updated-By:support@voxel.net

contact:POC-Name:Harold Finkbeiner

contact:POC-Email:harold.finkbeiner@neustar.biz

contact:POC-Phone:650-528-3731

contact:Tech-Name:Harold Finkbeiner

contact:Tech-Email:harold.finkbeiner@neustar.biz

contact:Tech-Phone:650-528-3731

contact:Abuse-Name:Voxel Abuse

contact:Abuse-Email:abuse@voxel.net

contact:Abuse-Phone:+1-212-812-4190

inetnum: 114.24.0.0 - 114.27.255.255

netname: HINET-NET

descr: CHTD, Chunghwa Telecom Co.,Ltd.

descr: No.21-3, Sec.1, Hsin-Yi Rd.

descr: Taipei Taiwan 100

country: TW

admin-c: FC76-AP

tech-c: HN27-AP

status: ALLOCATED PORTABLE

mnt-by: MAINT-TW-TWNIC

mnt-lower: MAINT-TW-TWNIC

mnt-routes: MAINT-TW-TWNIC

changed: hm-changed@apnic.net 20080418

source: APNIC

person: Fu-Kuei Chung

address: Internet Service Department,

address: Data Communication Business Group, Chunghwa Telecom Co., Ltd.

address: Data-Comm Bldg, No. 21, Sec 1, Hsin-Yi Rd.

address: Taipei, Taiwan 100

country: TW

phone: +886 2 2344 4709

phone: +886 2 2344 3007

fax-no: +886 2 2396 0399

fax-no: +886 2 2344 2513

e-mail: fkchung@ms1.hinet.net

nic-hdl: FC76-AP

mnt-by: MAINT-TW-TWNIC

changed: hostmaster@twnic.net 20001230

source: APNIC

person: HINET Network-Adm

address: CHTD, Chunghwa Telecom Co., Ltd.

address: No. 21, Sec. 21, Hsin-Yi Rd.,

address: Taipei Taiwan 100

country: TW

phone: +886 2 2322 3495

phone: +886 2 2322 3442

phone: +886 2 2344 3007

fax-no: +886 2 2344 2513

fax-no: +886 2 2395 5671

e-mail: network-adm@hinet.net

nic-hdl: HN27-AP

mnt-by: MAINT-TW-TWNIC

changed: hostmaster@twnic.net 20110822

source: APNIC

inetnum: 114.26.0.0 - 114.26.255.255

netname: HINET-NET

descr: Taipei Taiwan

country: TW

admin-c: HN184-TW

tech-c: HN184-TW

mnt-by: MAINT-TW-TWNIC

changed: network-adm@hinet.net 20080421

status: ASSIGNED NON-PORTABLE

source: TWNIC

person: HINET Network-Adm

address: CHTD, Chunghwa Telecom Co., Ltd.

address: Data-Bldg. 6F, No. 21, Sec. 21, Hsin-Yi Rd.,

address: Taipei Taiwan

country: TW

phone: +886-2-2322-3495

phone: +886-2-2322-3442

phone: +886-2-2344-3007

fax-no: +886-2-2344-2513

fax-no: +886-2-2395-5671

e-mail: network-adm@hinet.net

nic-hdl: HN184-TW

changed: hostmaster@twnic.net 20000721

source: TWNIC

NetRange: 128.59.0.0 - 128.59.255.255

CIDR: 128.59.0.0/16

OriginAS:

NetName: CU-NET

NetHandle: NET-128-59-0-0-1

Parent: NET-128-0-0-0-0

NetType: Direct Assignment

RegDate: 1985-02-05

Updated: 2008-12-12

Ref: http://whois.arin.net/rest/net/NET-128-59-0-0-1

OrgName: Columbia University

OrgId: COLUMB

Address: 612 W 115TH ST

City: NEW YORK

StateProv: NY

PostalCode: 10025

Country: US

RegDate:

Updated: 2008-12-12

Ref: http://whois.arin.net/rest/org/COLUMB

OrgAbuseHandle: CUAC-ARIN

OrgAbuseName: COLUMBIA UNIVERSITY ABUSE CONTACT

OrgAbusePhone: +1-212-854-1919

OrgAbuseEmail: abuse@columbia.edu

OrgAbuseRef: http://whois.arin.net/rest/poc/CUAC-ARIN

OrgTechHandle: CU-NOC-ARIN

OrgTechName: Columbia University Computer Operations

OrgTechPhone: +1-212-662-6442

OrgTechEmail: noc@columbia.edu

OrgTechRef: http://whois.arin.net/rest/poc/CU-NOC-ARIN

RTechHandle: CU-NOC-ARIN

RTechName: Columbia University Computer Operations

RTechPhone: +1-212-662-6442

RTechEmail: noc@columbia.edu

RTechRef: http://whois.arin.net/rest/poc/CU-NOC-ARIN

NetRange: 168.61.0.0 - 168.63.255.255

CIDR: 168.61.0.0/16, 168.62.0.0/15

OriginAS:

NetName: MSFT-EP

NetHandle: NET-168-61-0-0-1

Parent: NET-168-0-0-0-0

NetType: Direct Assignment

RegDate: 2011-06-22

Updated: 2012-10-16

Ref: http://whois.arin.net/rest/net/NET-168-61-0-0-1

OrgName: Microsoft Corp

OrgId: MSFT-Z

Address: One Microsoft Way

City: Redmond

StateProv: WA

PostalCode: 98052

Country: US

RegDate: 2011-06-22

Updated: 2011-06-22

Ref: http://whois.arin.net/rest/org/MSFT-Z

OrgAbuseHandle: MSNAB-ARIN

OrgAbuseName: MSN ABUSE

OrgAbusePhone: +1-425-882-8080

OrgAbuseEmail: abuse@msn.com

OrgAbuseRef: http://whois.arin.net/rest/poc/MSNAB-ARIN

OrgNOCHandle: ZM23-ARIN

OrgNOCName: Microsoft Corporation

OrgNOCPhone: +1-425-882-8080

OrgNOCEmail: noc@microsoft.com

OrgNOCRef: http://whois.arin.net/rest/poc/ZM23-ARIN

OrgAbuseHandle: HOTMA-ARIN

OrgAbuseName: Hotmail Abuse

OrgAbusePhone: +1-425-882-8080

OrgAbuseEmail: abuse@hotmail.com

OrgAbuseRef: http://whois.arin.net/rest/poc/HOTMA-ARIN

OrgTechHandle: MSFTP-ARIN

OrgTechName: MSFT-POC

OrgTechPhone: +1-425-882-8080

OrgTechEmail: iprrms@microsoft.com

OrgTechRef: http://whois.arin.net/rest/poc/MSFTP-ARIN

OrgAbuseHandle: ABUSE231-ARIN

OrgAbuseName: Abuse

OrgAbusePhone: +1-425-882-8080

OrgAbuseEmail: abuse@microsoft.com

OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE231-ARIN

NetRange: 173.160.0.0 - 173.167.255.255

CIDR: 173.160.0.0/13

OriginAS:

NetName: CBC-CM-4

NetHandle: NET-173-160-0-0-1

Parent: NET-173-0-0-0-0

NetType: Direct Allocation

RegDate: 2009-04-10

Updated: 2012-03-02

Ref: http://whois.arin.net/rest/net/NET-173-160-0-0-1

OrgName: Comcast Business Communications, LLC

OrgId: CBCI

Address: 1800 Bishops Gate Blvd.

City: Mount Laurel

StateProv: NJ

PostalCode: 08054-4628

Country: US

RegDate: 2001-12-21

Updated: 2011-01-06

Ref: http://whois.arin.net/rest/org/CBCI

OrgTechHandle: IC161-ARIN

OrgTechName: Comcast Cable Communications Inc

OrgTechPhone: +1-856-317-7200

OrgTechEmail: CNIPEO-Ip-registration@cable.comcast.com

OrgTechRef: http://whois.arin.net/rest/poc/IC161-ARIN

OrgAbuseHandle: NAPO-ARIN

OrgAbuseName: Network Abuse and Policy Observance

OrgAbusePhone: +1-856-317-7272

OrgAbuseEmail: abuse@comcast.net

OrgAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

RAbuseHandle: NAPO-ARIN

RAbuseName: Network Abuse and Policy Observance

RAbusePhone: +1-856-317-7272

RAbuseEmail: abuse@comcast.net

RAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

RTechHandle: IC161-ARIN

RTechName: Comcast Cable Communications Inc

RTechPhone: +1-856-317-7200

RTechEmail: CNIPEO-Ip-registration@cable.comcast.com

RTechRef: http://whois.arin.net/rest/poc/IC161-ARIN

NetRange: 173.162.128.0 - 173.162.255.255

CIDR: 173.162.128.0/17

OriginAS:

NetName: CBC-NEW-ENGLAND-15

NetHandle: NET-173-162-128-0-1

Parent: NET-173-160-0-0-1

NetType: Reallocated

RegDate: 2009-09-23

Updated: 2009-09-23

Ref: http://whois.arin.net/rest/net/NET-173-162-128-0-1

OrgName: Comcast Business Communications, LLC

OrgId: CBCI

Address: 1800 Bishops Gate Blvd.

City: Mount Laurel

StateProv: NJ

PostalCode: 08054-4628

Country: US

RegDate: 2001-12-21

Updated: 2011-01-06

Ref: http://whois.arin.net/rest/org/CBCI

OrgTechHandle: IC161-ARIN

OrgTechName: Comcast Cable Communications Inc

OrgTechPhone: +1-856-317-7200

OrgTechEmail: CNIPEO-Ip-registration@cable.comcast.com

OrgTechRef: http://whois.arin.net/rest/poc/IC161-ARIN

OrgAbuseHandle: NAPO-ARIN

OrgAbuseName: Network Abuse and Policy Observance

OrgAbusePhone: +1-856-317-7272

OrgAbuseEmail: abuse@comcast.net

OrgAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

RAbuseHandle: NAPO-ARIN

RAbuseName: Network Abuse and Policy Observance

RAbusePhone: +1-856-317-7272

RAbuseEmail: abuse@comcast.net

RAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

inetnum: 186.188.128/17

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

created: 20101210

changed: 20101210

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: 190.192/15

status: allocated

aut-num: N/A

owner: Prima S.A.

ownerid: AR-PRSA-LACNIC

responsible: Pablo Crespo

address: Hornos, 690,

address: C1272ACL - Buenos Aires -

country: AR

phone: +54 11 51996100 []

owner-c: MIF

tech-c: NEA

abuse-c: MIF

inetrev: 190.192/15

nserver: O200.PRIMA.COM.AR

nsstat: 20130226 AA

nslastaa: 20130226

nserver: O2000.PRIMA.COM.AR

nsstat: 20130226 AA

nslastaa: 20130226

created: 20090202

changed: 20090212

nic-hdl: MIF

person: Pablo Crespo

e-mail: lacnic@CABLEVISION.COM.AR

address: Hornos, 690,

address: C1272ACL - Capital Federal - BA

country: AR

phone: +54 11 51996100 []

created: 20021105

changed: 20120621

nic-hdl: NEA

person: Network Administrator

e-mail: lacnic@CABLEVISION.COM.AR

address: Aguero, 3440, 2 Piso

address: 1605 - Munro - BA

country: AR

phone: +54 11 47786569 []

created: 20030204

changed: 20120621

inetnum: 190.192/15

status: allocated

aut-num: N/A

owner: Prima S.A.

ownerid: AR-PRSA-LACNIC

responsible: Pablo Crespo

address: Hornos, 690,

address: C1272ACL - Buenos Aires -

country: AR

phone: +54 11 51996100 []

owner-c: MIF

tech-c: NEA

abuse-c: MIF

inetrev: 190.192/15

nserver: O200.PRIMA.COM.AR

nsstat: 20130226 AA

nslastaa: 20130226

nserver: O2000.PRIMA.COM.AR

nsstat: 20130226 AA

nslastaa: 20130226

created: 20090202

changed: 20090212

nic-hdl: MIF

person: Pablo Crespo

e-mail: lacnic@CABLEVISION.COM.AR

address: Hornos, 690,

address: C1272ACL - Capital Federal - BA

country: AR

phone: +54 11 51996100 []

created: 20021105

changed: 20120621

nic-hdl: NEA

person: Network Administrator

e-mail: lacnic@CABLEVISION.COM.AR

address: Aguero, 3440, 2 Piso

address: 1605 - Munro - BA

country: AR

phone: +54 11 47786569 []

created: 20030204

changed: 20120621

NetRange: 192.69.88.0 - 192.69.95.255

CIDR: 192.69.88.0/21

OriginAS: AS46664

NetName: VOLUM-ARIN

NetHandle: NET-192-69-88-0-1

Parent: NET-192-0-0-0-0

NetType: Direct Allocation

RegDate: 2013-01-03

Updated: 2013-01-03

Ref: http://whois.arin.net/rest/net/NET-192-69-88-0-1

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: 198.24.128.0 - 198.24.191.255

CIDR: 198.24.128.0/18

OriginAS: AS20454, AS32164

NetName: SECUREDSERVERS

NetHandle: NET-198-24-128-0-1

Parent: NET-198-0-0-0-0

NetType: Direct Allocation

RegDate: 2012-10-30

Updated: 2012-10-30

Ref: http://whois.arin.net/rest/net/NET-198-24-128-0-1

OrgName: SECURED SERVERS LLC

OrgId: SSL-65

Address: 2353 W University Bldg A

City: Tempe

StateProv: AZ

PostalCode: 85281

Country: US

RegDate: 2003-12-08

Updated: 2012-03-13

Ref: http://whois.arin.net/rest/org/SSL-65

ReferralServer: rwhois://rwhois.securedservers.com:4321

OrgAbuseHandle: ABUSE1536-ARIN

OrgAbuseName: Abuse

OrgAbusePhone: +1-480-422-2022

OrgAbuseEmail: abuse@securedservers.com

OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE1536-ARIN

OrgTechHandle: IPADM294-ARIN

OrgTechName: IPADMIN

OrgTechPhone: +1-480-422-2031

OrgTechEmail: ipadmin@securedservers.com

OrgTechRef: http://whois.arin.net/rest/poc/IPADM294-ARIN

Found a referral to rwhois.securedservers.com:4321.

autharea=198.24.160.0/19

xautharea=198.24.160.0/19

network:Class-Name:network

network:Auth-Area:198.24.160.0/19

network:ID:NET-38977.198.24.160.40/29

network:Network-Name:Public

network:IP-Network:198.24.160.40/29

network:IP-Network-Block:198.24.160.40 - 198.24.160.47

network:Org-Name:EyeOfEnder

network:Street-Address:116 Stapley Road

network:City:Brighton and Hove

network:State:BNH

network:Postal-Code:BN37FG

network:Country-Code:GB

network:Tech-Contact:MAINT-38977.198.24.160.40/29

network:Created:20130208184201000

network:Updated:20130208184201000

network:Updated-By:dnsadmin@securedservers.com

contact:POC-Name:DNS Administrator

contact:POC-Email:dnsadmin@securedservers.com

contact:POC-Phone:(480) 422-2023

contact:Tech-Name:DNS Administrator

contact:Tech-Email:dnsadmin@securedservers.com

contact:Tech-Phone:(480) 422-2023

contact:Abuse-Name:Abuse

contact:Abuse-Email:abuse@securedservers.com

contact:Abuse-Phone:+1-480-422-2022 (Office)

inetnum: 200.25.146/23

status: reallocated

owner: Satnet Gye Coorp

ownerid: EC-SGCO-LACNIC

responsible: Christian Francis

address: Juan Tanca Marengo Km 2.5, s/n,

address: 0901 - Guayaquil - Gu

country: EC

phone: +593 4 6004400 [319]

owner-c: JOC

tech-c: JOC

abuse-c: JOC

inetrev: 200.25.146/23

nserver: UIO2.SATNET.NET

nsstat: 20130305 AA

nslastaa: 20130305

nserver: GYE2.SATNET.NET

nsstat: 20130305 AA

nslastaa: 20130305

created: 20110216

changed: 20110216

inetnum-up: 200.25.144/21

inetnum-up: 200.25.128/19

nic-hdl: JOC

person: Christian Francis

e-mail: cfrancis@GYE.SATNET.NET

address: Av. Juan Tanca Marengo Km 2.5, as, 14522

address: 0901 - Guayaquil - GU

country: EC

phone: +593 4 6002400 [1334]

created: 20021211

changed: 20121120

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: 20130303 AA

nslastaa: 20130303

nserver: NS2.PSINETPA.NET

nsstat: 20130303 AA

nslastaa: 20130303

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: 200.84.192/18

status: allocated

aut-num: N/A

owner: CANTV Servicios, Venezuela

ownerid: VE-CSVE-LACNIC

responsible: Nicolas Ortiz

address: Segunda Avenida de los Palos Grandes, 000, Entre Av. Fr

address: 1060 - Caracas - MI

country: VE

phone: +58 212 2095680 []

owner-c: LUM

tech-c: LUM

abuse-c: LUM

inetrev: 200.84.192/18

nserver: DNS1.CANTV.NET

nsstat: 20130303 AA

nslastaa: 20130303

nserver: DNS2.CANTV.NET

nsstat: 20130303 AA

nslastaa: 20130303

created: 20021031

changed: 20021031

nic-hdl: LUM

person: Nicolas Ortiz

e-mail: ipadmin@CANTV.NET

address: Segunda Avenida de los Palos Grandes, Entre Av. Fr, 000,

address: 1060 - Caracas - MI

country: VE

phone: +58 212 2095680 []

created: 20020911

changed: 20121108

inetnum: 46.4.94.128 - 46.4.94.159

netname: HETZNER-RZ14

descr: Hetzner Online AG

descr: Datacenter 14

country: DE

admin-c: HOAC1-RIPE

tech-c: HOAC1-RIPE

status: ASSIGNED PA

mnt-by: HOS-GUN

mnt-lower: HOS-GUN

mnt-routes: HOS-GUN

role: Hetzner Online AG - Contact Role

address: Hetzner Online AG

address: Stuttgarter Strasse 1

address: D-91710 Gunzenhausen

address: Germany

phone: +49 9831 61 00 61

fax-no: +49 9831 61 00 62

abuse-mailbox: abuse@hetzner.de

org: ORG-HOA1-RIPE

admin-c: MH375-RIPE

tech-c: GM834-RIPE

tech-c: SK2374-RIPE

tech-c: TF2013-RIPE

tech-c: MF1400-RIPE

tech-c: SK8441-RIPE

nic-hdl: HOAC1-RIPE

mnt-by: HOS-GUN

route: 46.4.0.0/16

descr: HETZNER-RZ-FKS-BLK3

origin: AS24940

org: ORG-HOA1-RIPE

mnt-by: HOS-GUN

organisation: ORG-HOA1-RIPE

org-name: Hetzner Online AG

org-type: LIR

address: Hetzner Online AG

address: Attn. Martin Hetzner

address: Stuttgarter Str. 1

address: 91710

address: Gunzenhausen

address: GERMANY

phone: +49 9831 610061

fax-no: +49 9831 610062

admin-c: TF2013-RIPE

admin-c: MF1400-RIPE

admin-c: GM834-RIPE

admin-c: HOAC1-RIPE

admin-c: MH375-RIPE

admin-c: SK8441-RIPE

admin-c: SK2374-RIPE

mnt-ref: HOS-GUN

mnt-ref: RIPE-NCC-HM-MNT

mnt-by: RIPE-NCC-HM-MNT

inetnum: 46.4.94.224 - 46.4.94.255

netname: HETZNER-RZ14

descr: Hetzner Online AG

descr: Datacenter 14

country: DE

admin-c: HOAC1-RIPE

tech-c: HOAC1-RIPE

status: ASSIGNED PA

mnt-by: HOS-GUN

mnt-lower: HOS-GUN

mnt-routes: HOS-GUN

role: Hetzner Online AG - Contact Role

address: Hetzner Online AG

address: Stuttgarter Strasse 1

address: D-91710 Gunzenhausen

address: Germany

phone: +49 9831 61 00 61

fax-no: +49 9831 61 00 62

abuse-mailbox: abuse@hetzner.de

org: ORG-HOA1-RIPE

admin-c: MH375-RIPE

tech-c: GM834-RIPE

tech-c: SK2374-RIPE

tech-c: TF2013-RIPE

tech-c: MF1400-RIPE

tech-c: SK8441-RIPE

nic-hdl: HOAC1-RIPE

mnt-by: HOS-GUN

route: 46.4.0.0/16

descr: HETZNER-RZ-FKS-BLK3

origin: AS24940

org: ORG-HOA1-RIPE

mnt-by: HOS-GUN

organisation: ORG-HOA1-RIPE

org-name: Hetzner Online AG

org-type: LIR

address: Hetzner Online AG

address: Attn. Martin Hetzner

address: Stuttgarter Str. 1

address: 91710

address: Gunzenhausen

address: GERMANY

phone: +49 9831 610061

fax-no: +49 9831 610062

admin-c: TF2013-RIPE

admin-c: MF1400-RIPE

admin-c: GM834-RIPE

admin-c: HOAC1-RIPE

admin-c: MH375-RIPE

admin-c: SK8441-RIPE

admin-c: SK2374-RIPE

mnt-ref: HOS-GUN

mnt-ref: RIPE-NCC-HM-MNT

mnt-by: RIPE-NCC-HM-MNT

inetnum: 62.75.178.0 - 62.75.178.255

netname: BSB-SERVICE-1

descr: BSB-SERVICE Dedicated Server Hosting

country: DE

org: ORG-BSBS1-RIPE

admin-c: NPA10-RIPE

tech-c: NPA10-RIPE

status: LIR-PARTITIONED 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: OHPS-RIPE

tech-c: CDPS-RIPE

tech-c: ADPS-RIPE

nic-hdl: NPA10-RIPE

mnt-by: INTERGENIA-MNT

route: 62.75.128.0/17

descr: Plusserver AG

origin: AS8972

mnt-by: INTERGENIA-MNT

mnt-lower: INTERGENIA-MNT

NetRange: 66.192.0.0 - 66.195.255.255

CIDR: 66.192.0.0/14

OriginAS:

NetName: TWTC-NETBLK-4

NetHandle: NET-66-192-0-0-1

Parent: NET-66-0-0-0-0

NetType: Direct Allocation

Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

RegDate: 2001-10-25

Updated: 2012-02-24

Ref: http://whois.arin.net/rest/net/NET-66-192-0-0-1

OrgName: tw telecom holdings, inc.

OrgId: TWTC

Address: 10475 Park Meadows Drive

City: Littleton

StateProv: CO

PostalCode: 80124

Country: US

RegDate: 1999-03-17

Updated: 2008-10-04

Ref: http://whois.arin.net/rest/org/TWTC

ReferralServer: rwhois://rwhois.twtelecom.net:4321

OrgAbuseHandle: TWTAD-ARIN

OrgAbuseName: tw telecom Abuse Desk

OrgAbusePhone: +1-800-898-6473

OrgAbuseEmail: abuse@twtelecom.net

OrgAbuseRef: http://whois.arin.net/rest/poc/TWTAD-ARIN

OrgNOCHandle: TDN1-ARIN

OrgNOCName: TWTC Data NOC

OrgNOCPhone: +1-800-898-6473

OrgNOCEmail: support@twtelecom.net

OrgNOCRef: http://whois.arin.net/rest/poc/TDN1-ARIN

OrgTechHandle: NST12-ARIN

OrgTechName: NOC SWIP Team

OrgTechPhone: +1-800-898-6473

OrgTechEmail: swip@twtelecom.com

OrgTechRef: http://whois.arin.net/rest/poc/NST12-ARIN

RTechHandle: ZT87-ARIN

RTechName: IP Manager

RTechPhone: +1-800-829-0420

RTechEmail: ipmanager@twtelecom.net

RTechRef: http://whois.arin.net/rest/poc/ZT87-ARIN

NetRange: 66.193.187.0 - 66.193.187.255

CIDR: 66.193.187.0/24

OriginAS:

NetName: TWTC-R2I-01

NetHandle: NET-66-193-187-0-1

Parent: NET-66-192-0-0-1

NetType: Reassigned

RegDate: 2004-01-27

Updated: 2004-01-27

Ref: http://whois.arin.net/rest/net/NET-66-193-187-0-1

OrgName: R2K INC

OrgId: R2KIN

Address: 83 MAIDEN LN

City: NEW YORK

StateProv: NY

PostalCode: 10038

Country: US

RegDate: 2004-01-27

Updated: 2011-09-24

Ref: http://whois.arin.net/rest/org/R2KIN

OrgAbuseHandle: RYI-ARIN

OrgAbuseName: YIEN, RICHARD

OrgAbusePhone: +1-212-440-1700

OrgAbuseEmail: RICHARD.YIEN@r2k.com

OrgAbuseRef: http://whois.arin.net/rest/poc/RYI-ARIN

OrgTechHandle: RYI-ARIN

OrgTechName: YIEN, RICHARD

OrgTechPhone: +1-212-440-1700

OrgTechEmail: RICHARD.YIEN@r2k.com

OrgTechRef: http://whois.arin.net/rest/poc/RYI-ARIN

Found a referral to rwhois.twtelecom.net:4321.

network:Class-Name:network

network:ID:f8122fd4-352f-11e0-94c6-0015c5e41ca0

network:Auth-Area:66.193.0.0/16

network:Network-Name:CDO-Technologies-66-193-187-128

network:IP-Network:66.193.187.128/25

network:Organization;I:e0c585a6-352f-11e0-a67b-0015c5e41ca0

network:Org-Name:CDO Technologies

network:Street-Address:5200 SPRINGFIELD ST

network:City:DAYTON

network:State:OH

network:Postal-Code:45431

network:Country-Code:us

network:Phone:none

network:Admin-Contact;I:none

network:Tech-Contact;I:none

network:Abuse-Contact;I:abuse@twtelecom.net

network:Updated:20110210090216000