www.glesec.com

GLESEC

Your Global e-security Partner

MONTHLY SECURITY REPORT

PREPARED FOR: METROBANK

JANUARY 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 of malware, phishing, organized crime, and hacktivism is the very cause of this of information security exposure phenomena.

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 JANUARY 1, 2013 to JANUARY 31, 2013

Based on the information gathered from the DefensePro during this period **9,254** attacks on METROBANK, **101** of which were considered critical were all stopped by the Radware DefensePro 508. During the previous period, 13,350 attacks on METROBANK, 207 of which were considered critical were all stopped by the Radware DefensePro 508. The overall quantity of attacks dropped compared to the previous period.

Similar to previous report periods GLESEC has discovered constant Brute Force Web, DNS, and SMB attacks. GLESEC observed most of the activity from IP Addresses known to be from the DoD Network Information Center. After further investigation one would come to the conclusion that IP spoofing would be the most likely cause of the attacks appearing to originate from the Department of Defense, an evasion tactic attackers use to hide their real location, but in fact METROBANK is utilizing public IPs on private segments. A query was presented to METROBANK as to reasoning behind such configuration.

Scanning attempts such as: TCP Scan (horizontal), TCP Scan (vertical), TCP Scan, Web Scan, UDP Scan (horizontal), UDP Scan (vertical), UDP Scan, Ping Sweep and SIP-Scanner-SIPVicious attempts were also frequent and are geographically most prevalent from Asia, specifically from China. Cracking and Anti Scanning Protection played a large part in defending the network and servers by dropping the malicious traffic. GLESEC discovered attacks directed at well-known port numbers: 443 (https), 25 (smtp), 1433 (microsoft-sql-server), 23 (telnet), 3306 (mysql), 22 (ssh), 5060 (sip), 3389 (rdp/ms wbt server), 8080 (http-alt), 80 (http), and 445 (microsoft-ds) in order of frequency. Microsoft SQL Server and MySQL were heavily probed and the services should be reviewed and hardened to prevent any further intrusion if they are in production.

As with previous report periods Flood attacks were common such as HTTP Page Flood, Network Flood utilizing IPv4 UDP attacks. Rate Limiting, Behavioral DoS, DoS Protection and Signature Protection assisted in mitigating these attack vectors.

Large numbers of “TCP handshake violation, first packet not syn” are being observed, triggering the device to block the anomalous traffic. This is caused by applications that do not adhere to RFC standards.

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 such as those observed originating from China.

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)

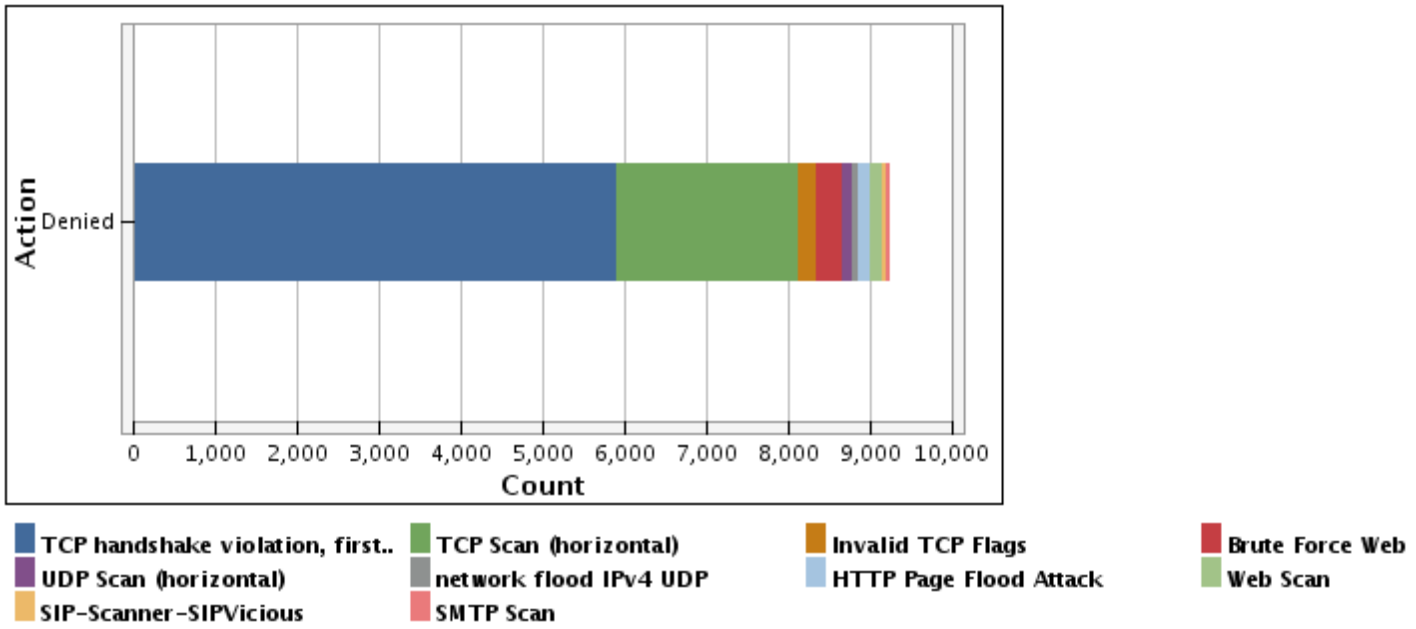
METROBANK Systems: Radware DefensePro 508

METROBANK Systems: Radware AppWall (Not 100% in production)

6. Detailed Security Report

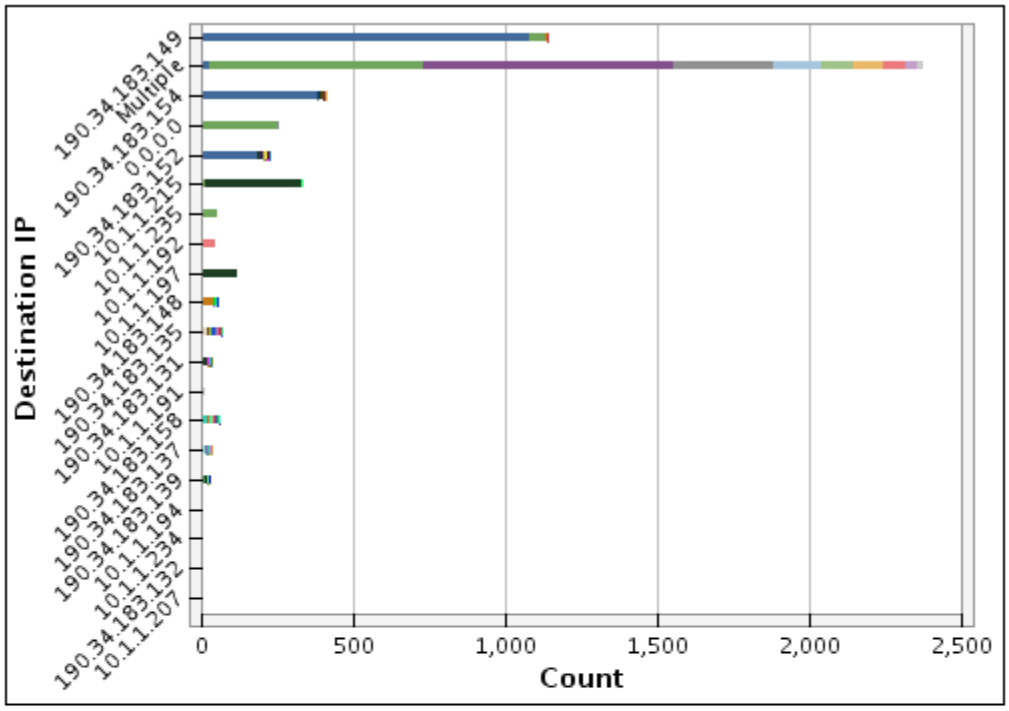
Graph: Attacks Allowed and Denied

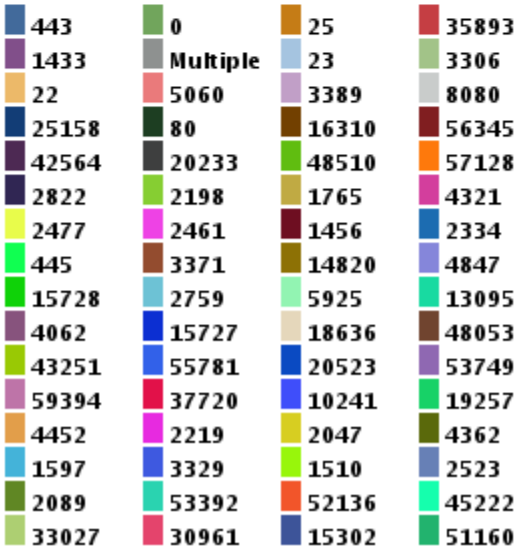
This report provides the count of total allowed and denied attacks along with network security rule.



Graph: Attacks by Destination and Port

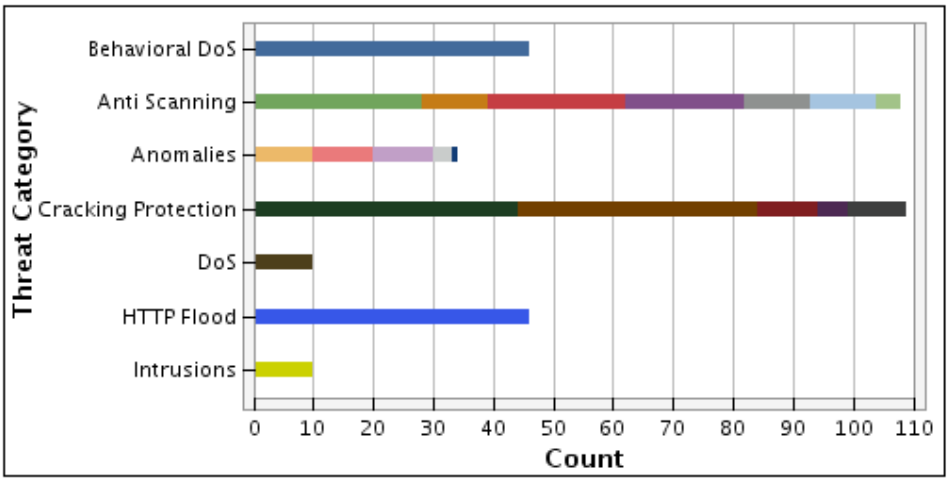
This report provides information on the total number of attacks that were attempted on which target device and port and for how many times, along with the attack name, network security rule.

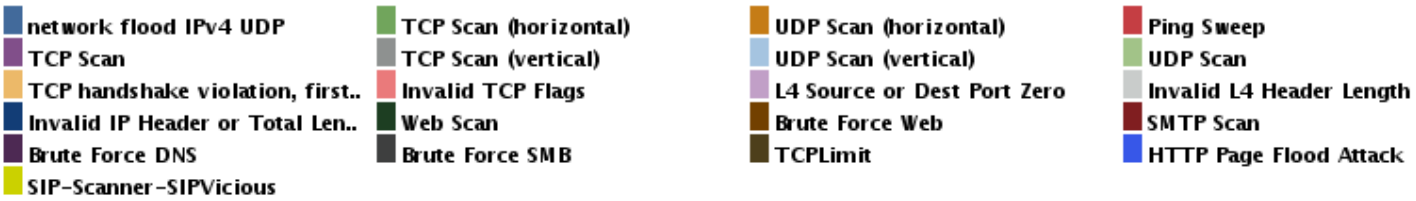




Graph: Attacks By Threat Category

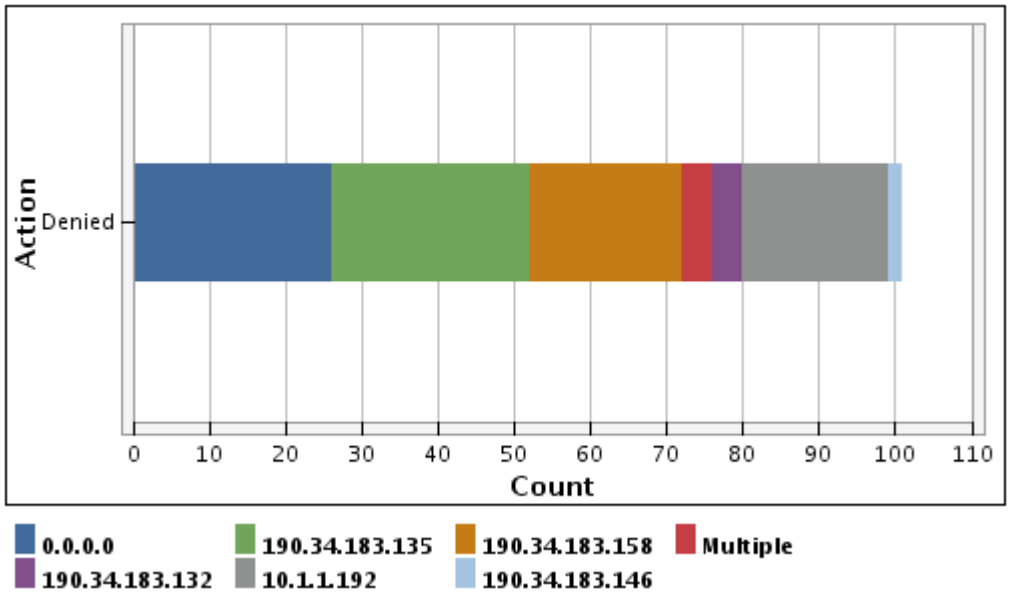
This report lists the attacks per Attack Category, listing the attack name, network security rule.





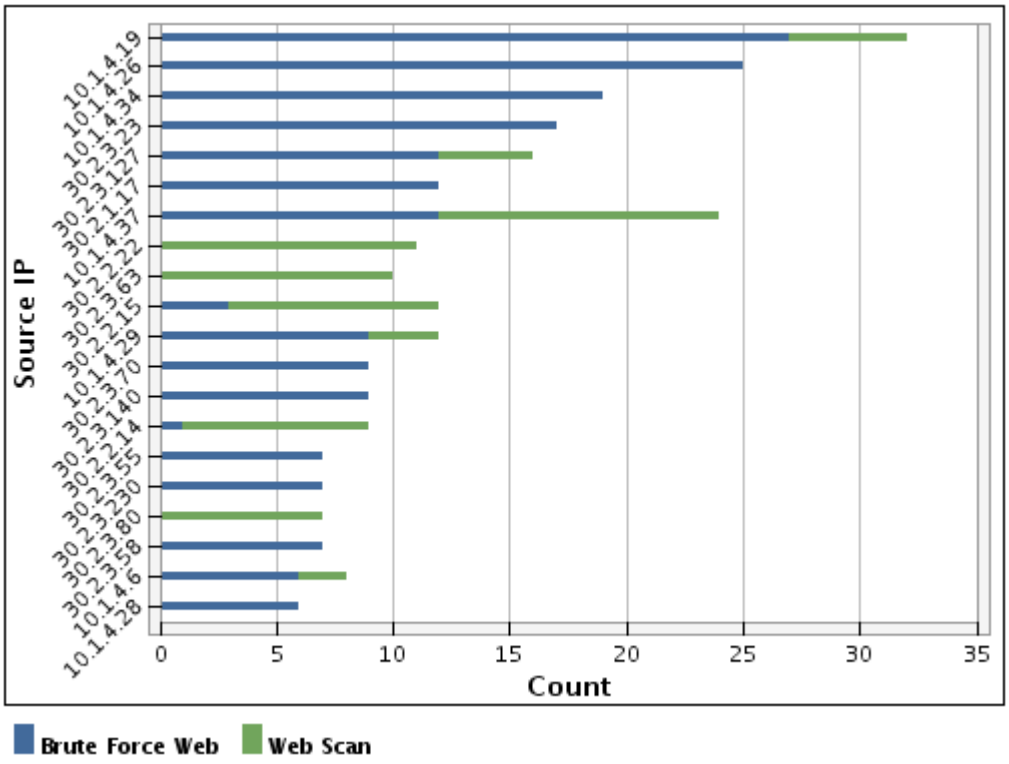
Graph: Critical Attacks

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.



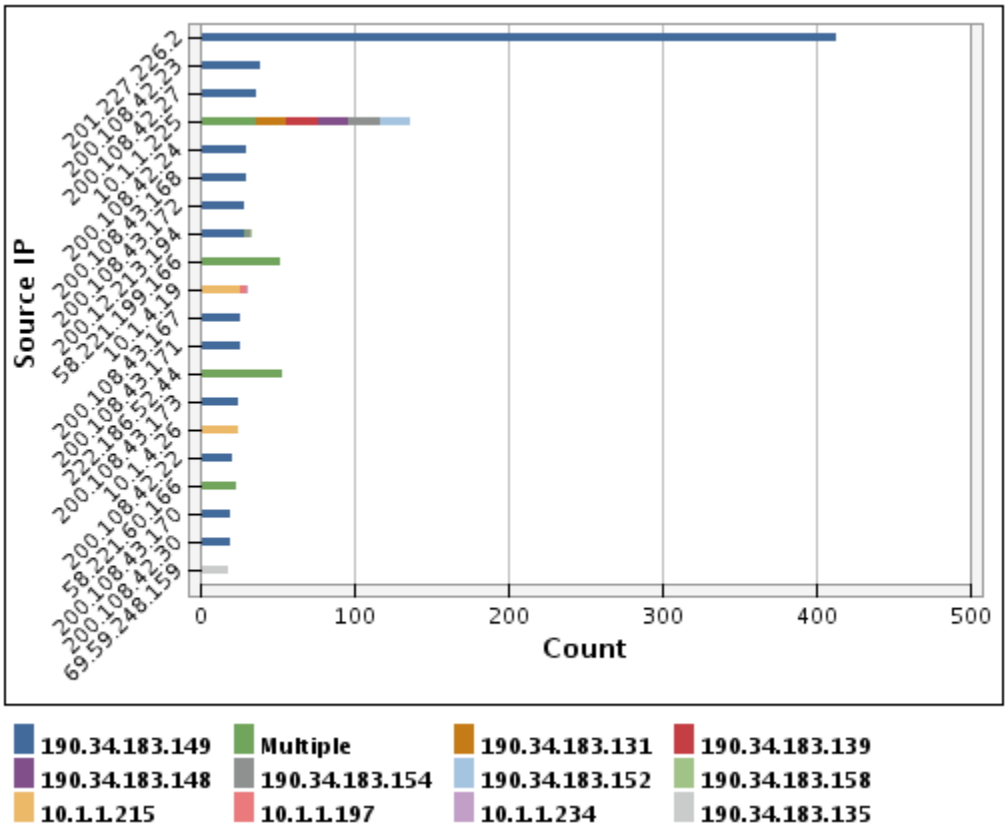
Graph: Internal Attacks by Sources

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.



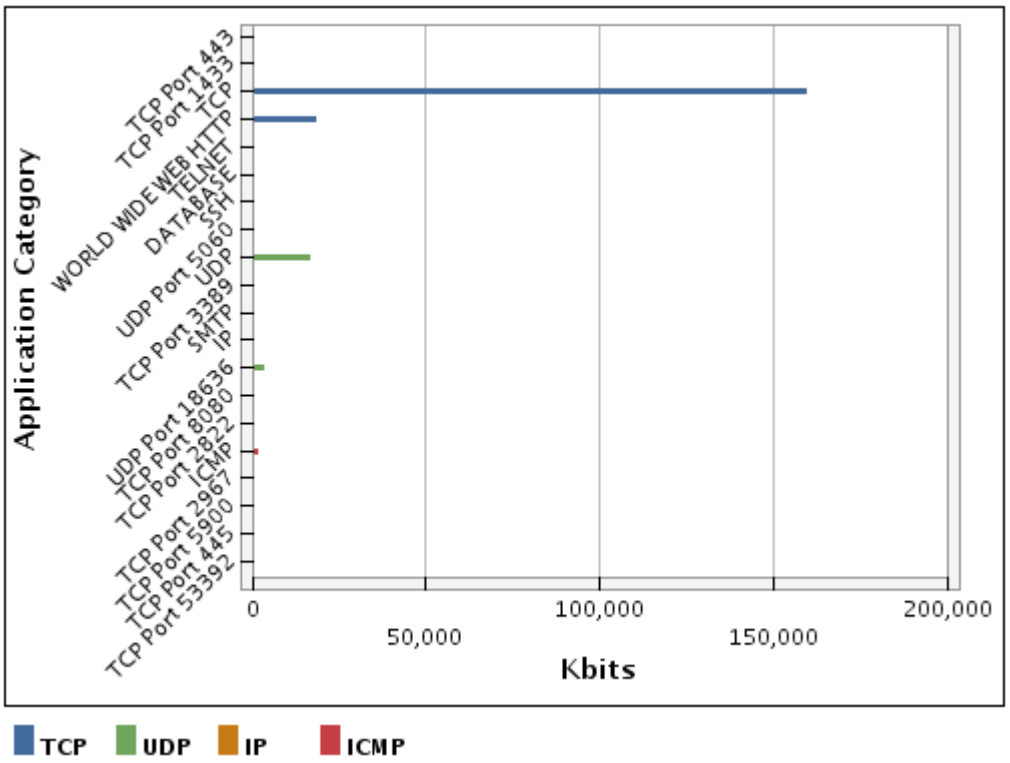
Graph: Top Attack Sources Blocked

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.



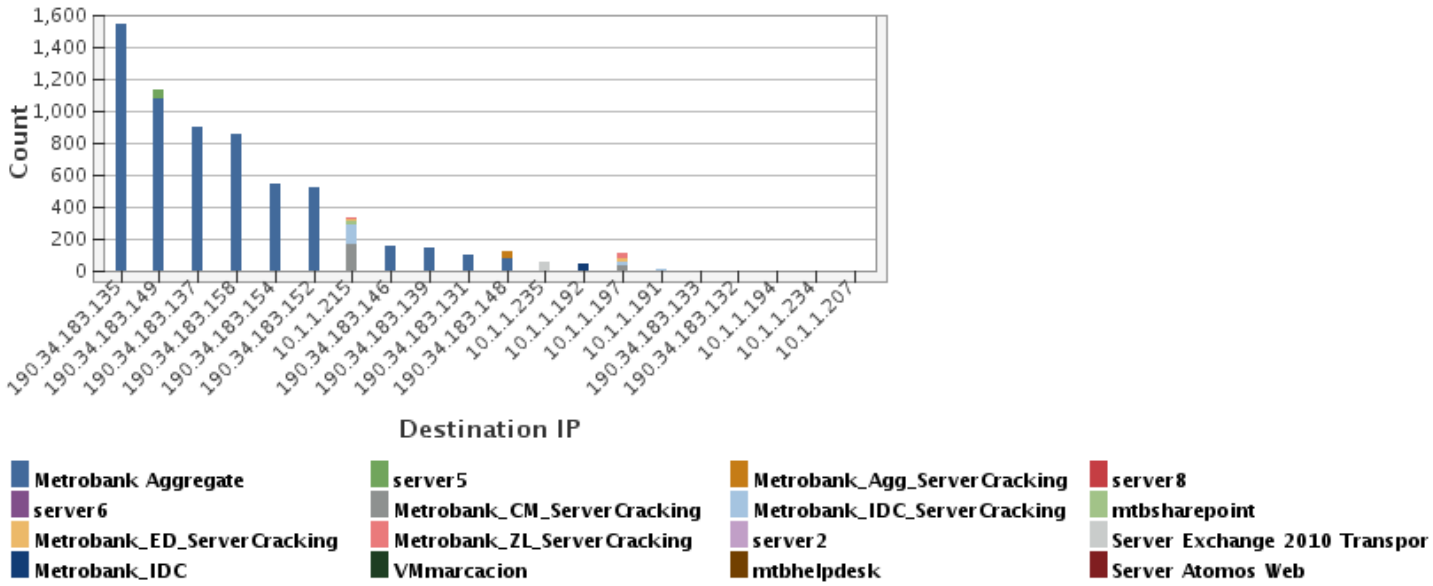
Graph: Top Attacked Applications

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).



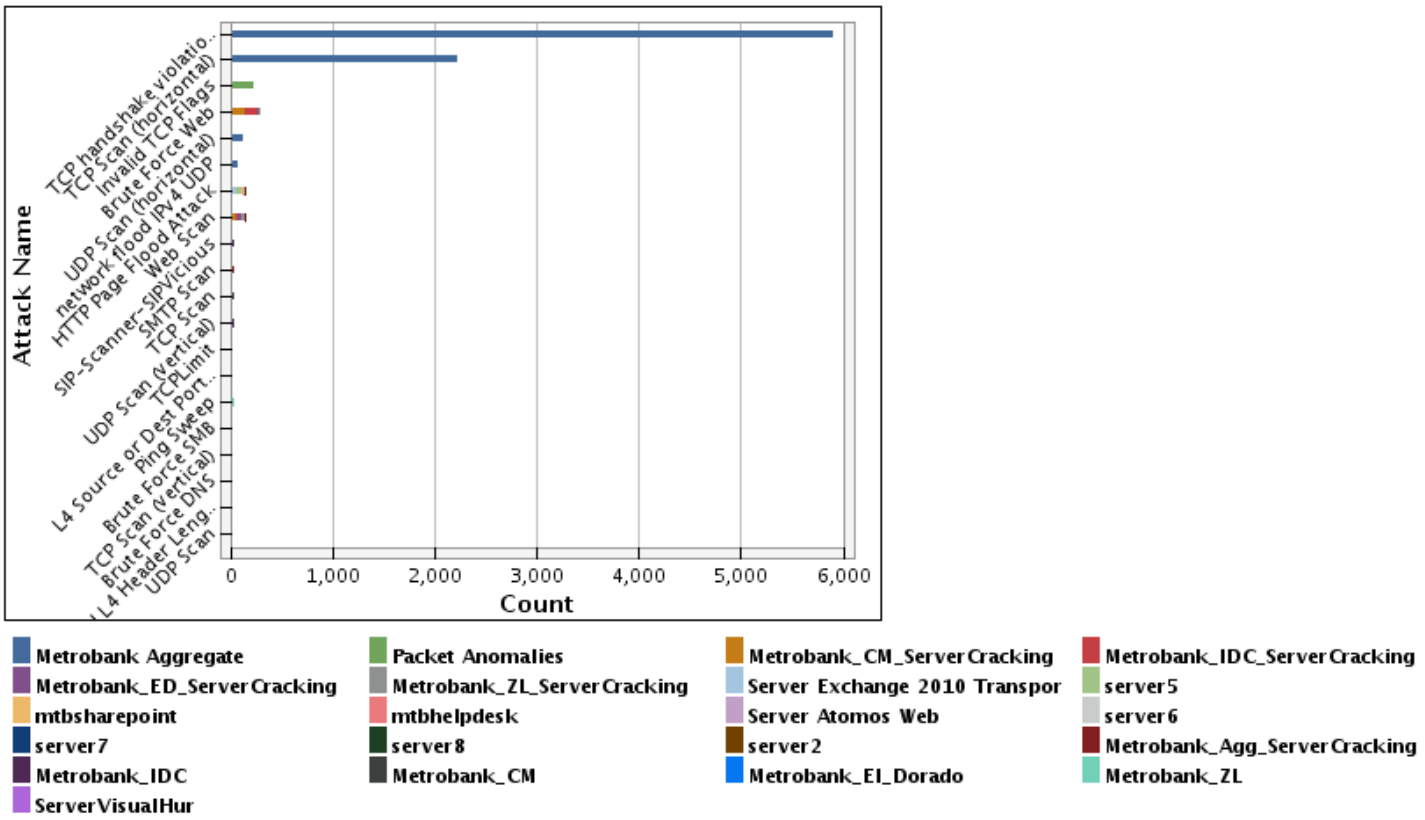
Graph: Top Attacked Destinations

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.



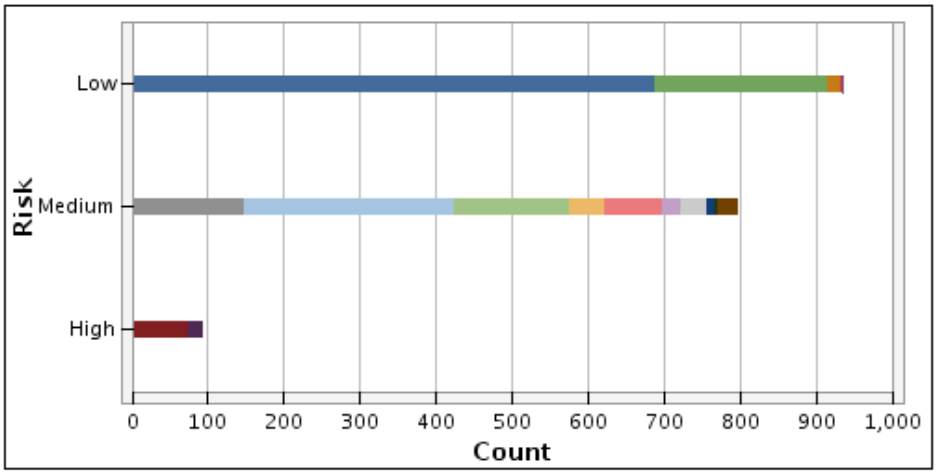
Graph: Top Attacks Blocked

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

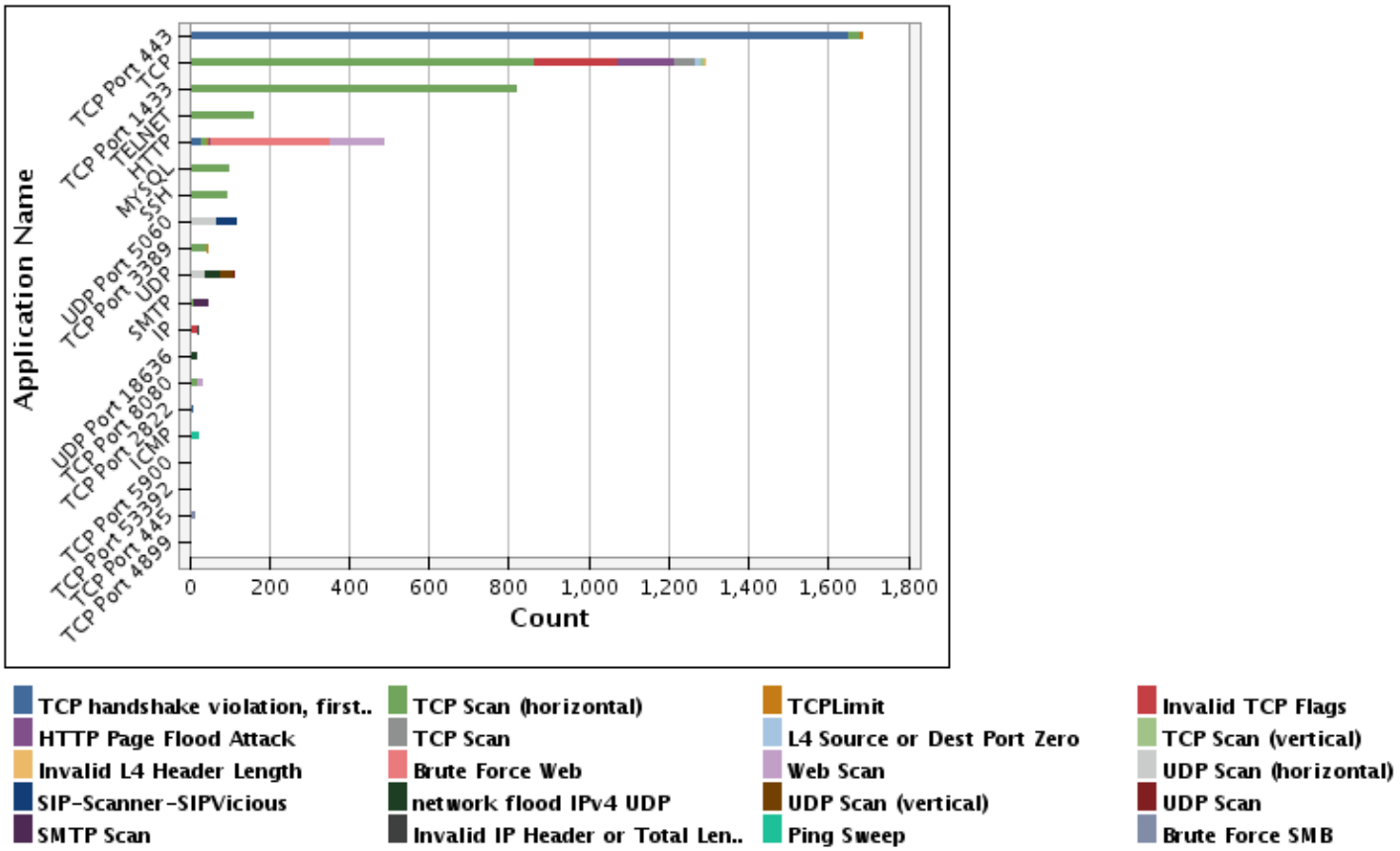
This report provides information on the attacks, which were blocked on DP IPS based on their risk. In this report the risk of the attack, attack name, source, destination, the destination port, network security rules are shown.



TCP handshake violation, first..
Invalid IP Header or Total Len..
TCP Scan
Brute Force SMB
SIP-Scanner-SIPVicious
Invalid TCP Flags
HTTP Page Flood Attack
Web Scan
Brute Force DNS
L4 Source or Dest Port Zero
TCP Scan (horizontal)
Ping Sweep
UDP Scan (vertical)
Invalid L4 Header Length
Brute Force Web
UDP Scan (horizontal)
network flood IPv4 UDP

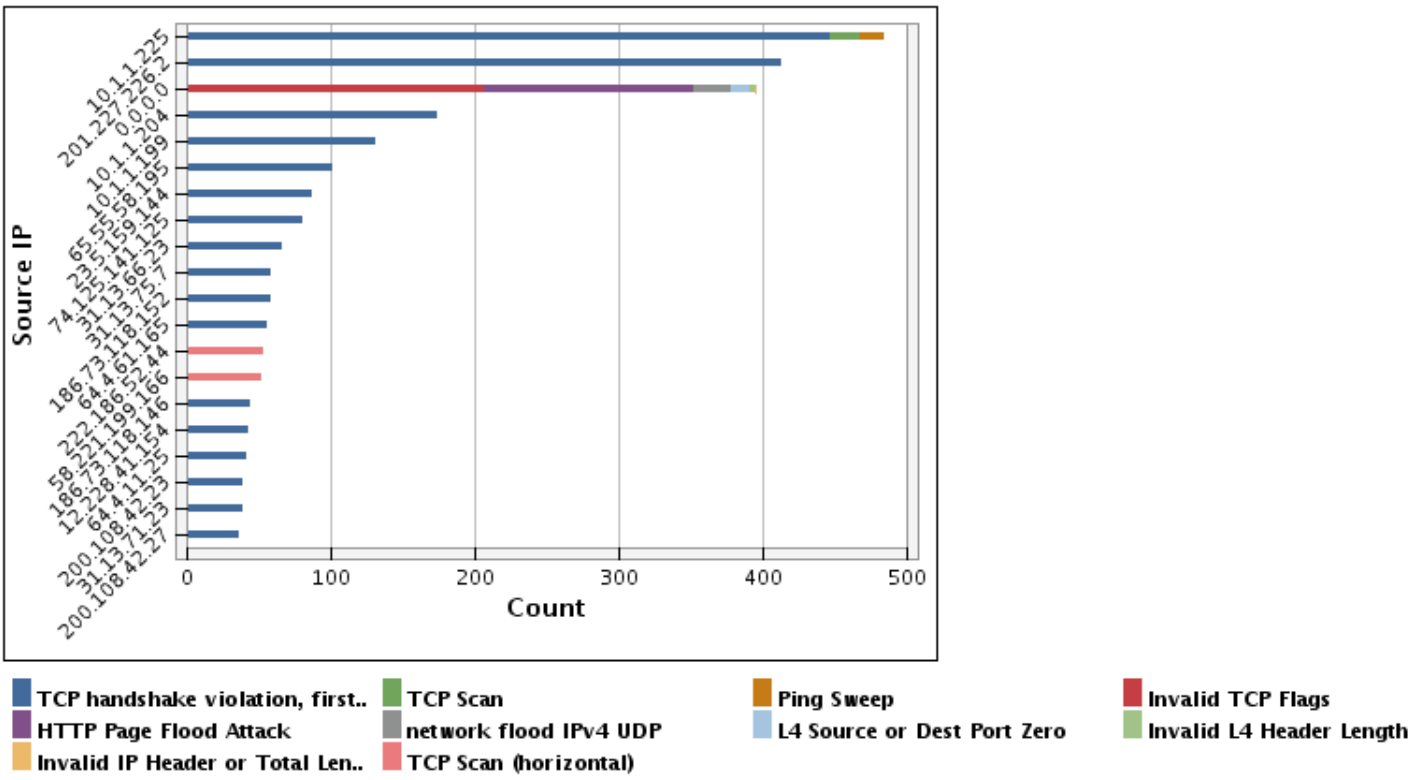
Graph: Top Attacks by Application

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.



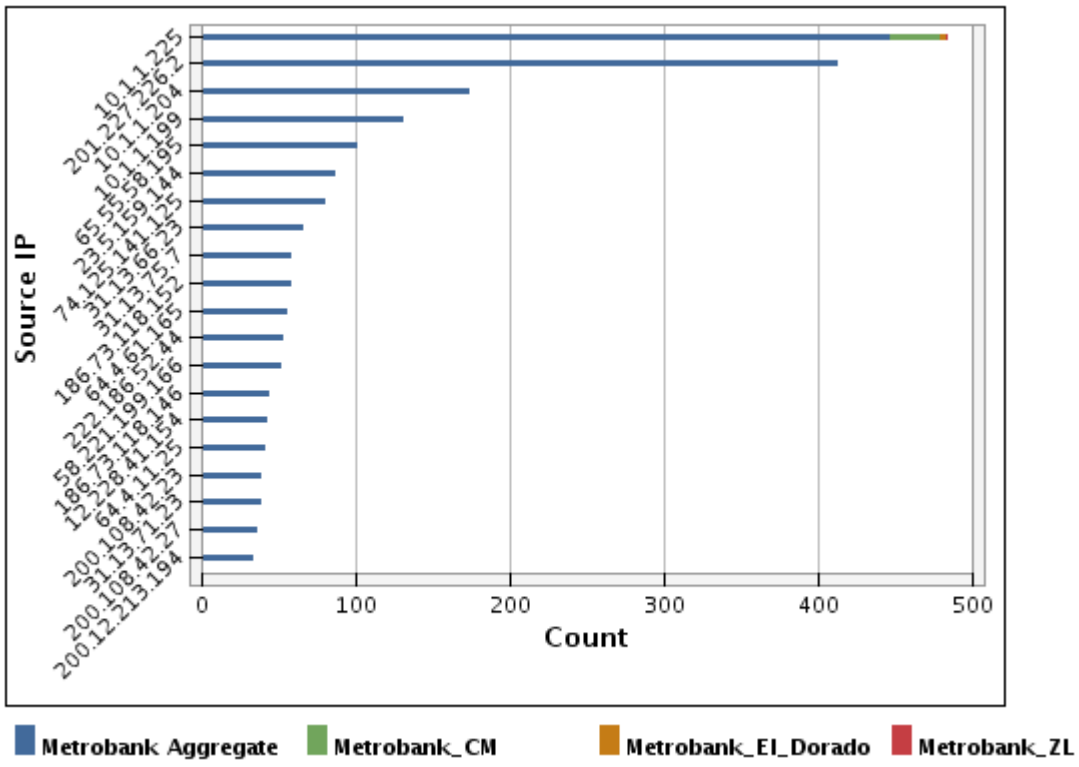
Graph: Top Attacks by Source

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.



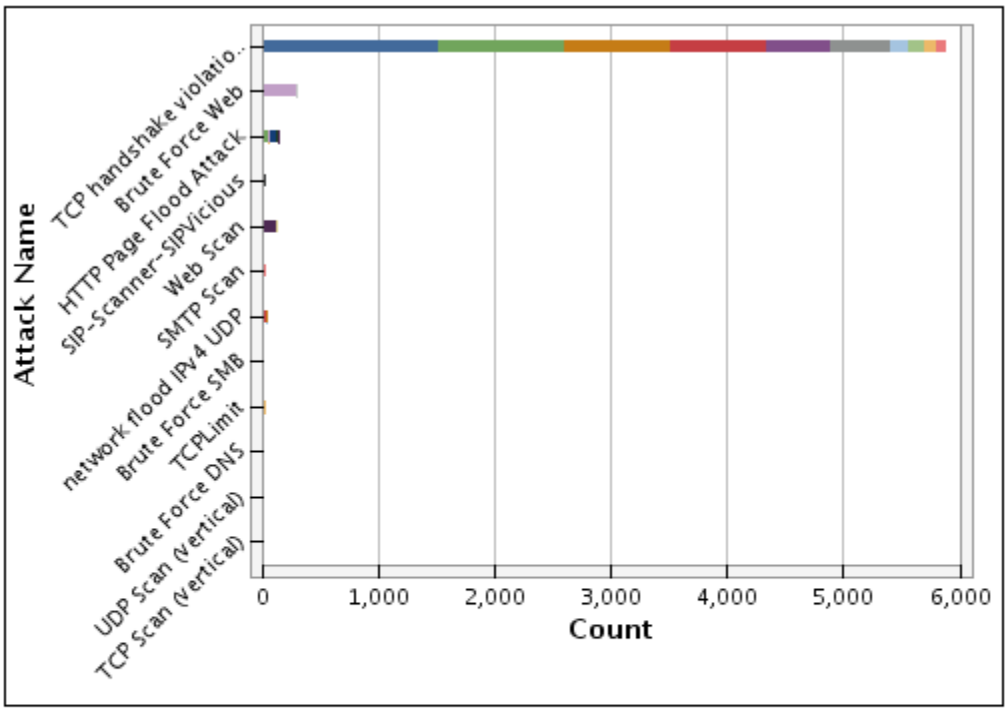
Graph: Top Denied Attackers

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'.



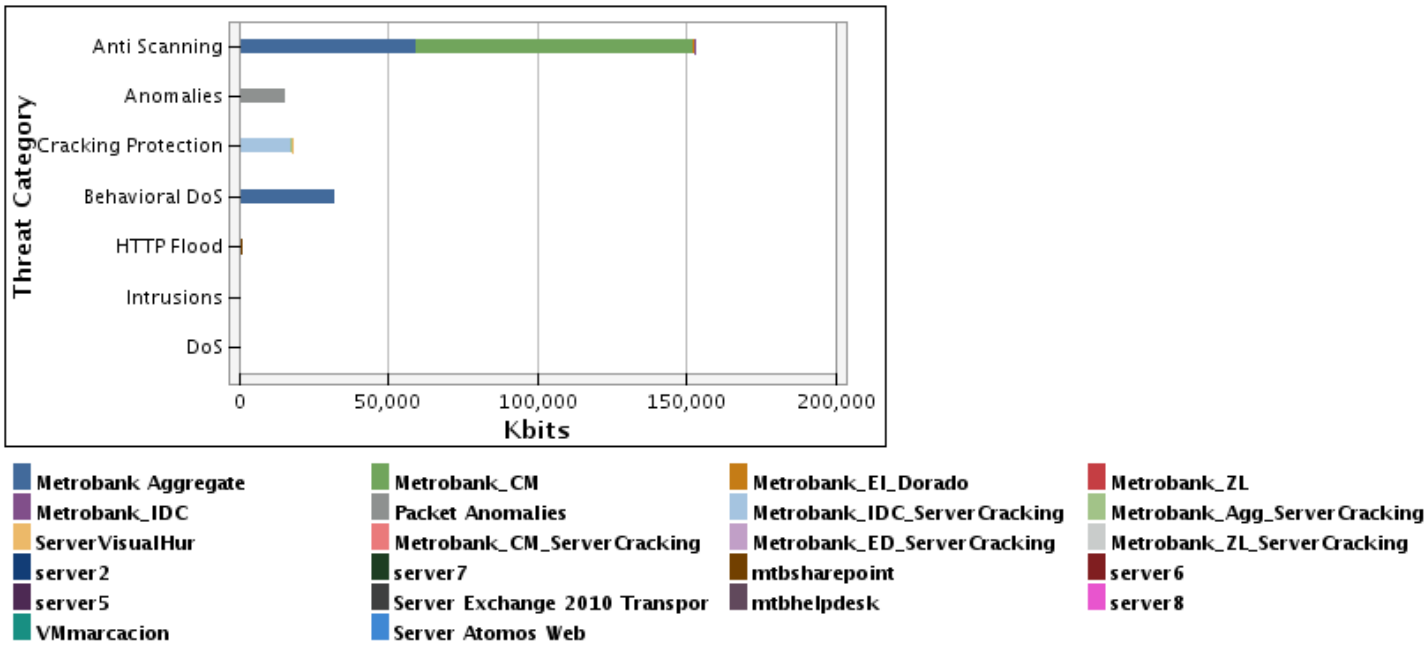
Graph: Top Destinations by Attack

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.



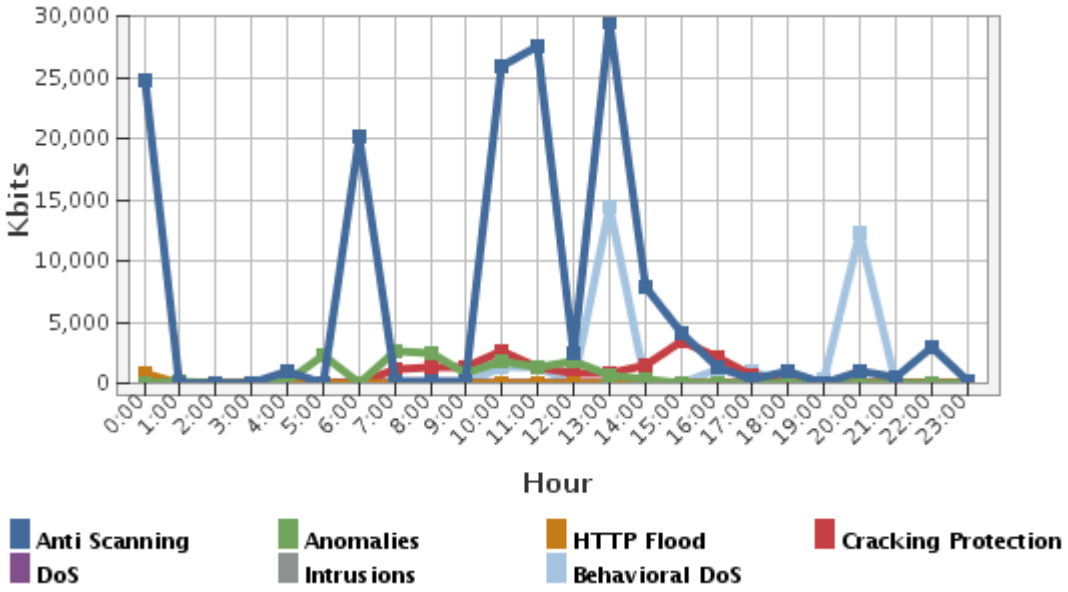
Graph: Attack Categories by Bandwidth

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.



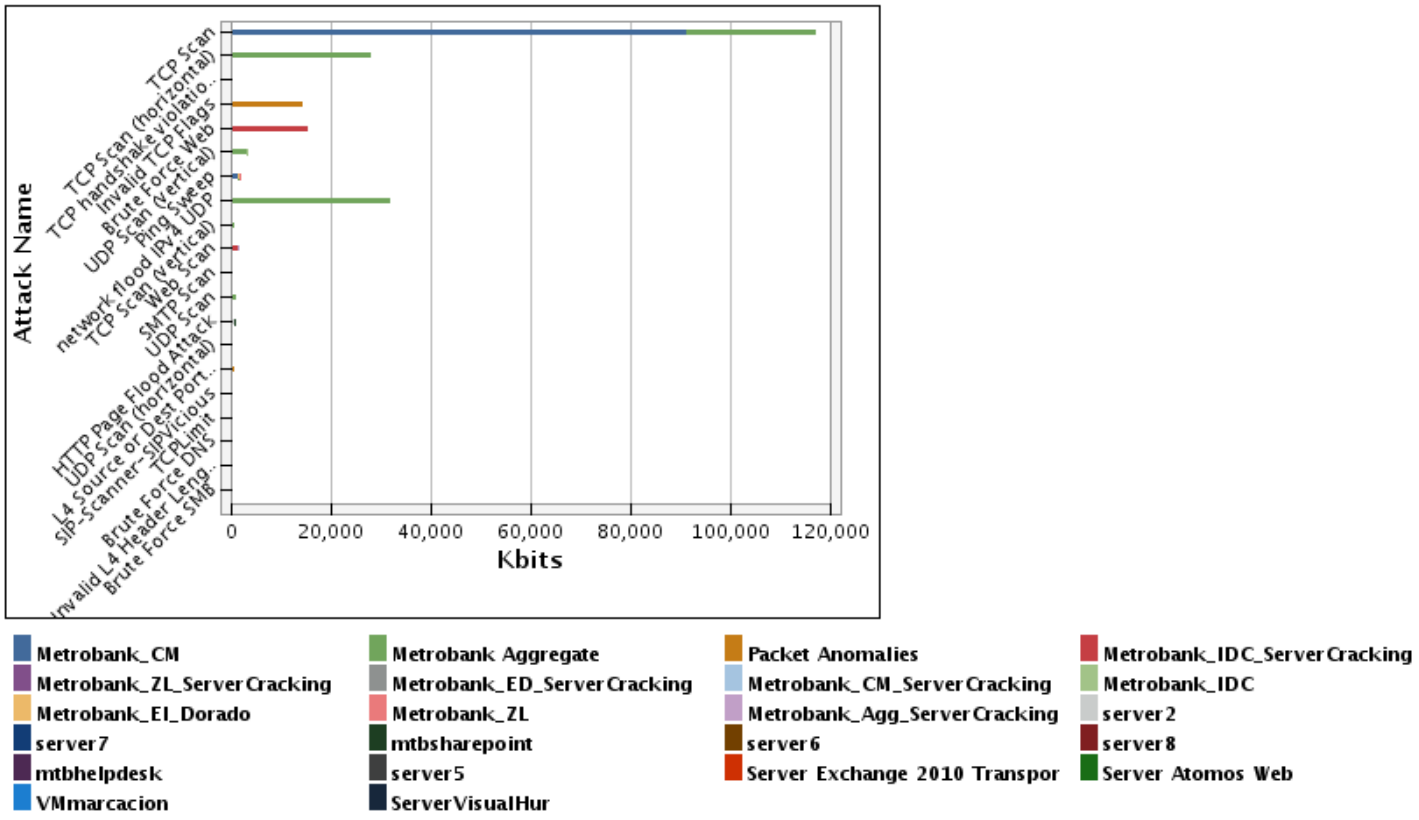
Graph: Bandwidth by Threat Category by Hour of Day

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.



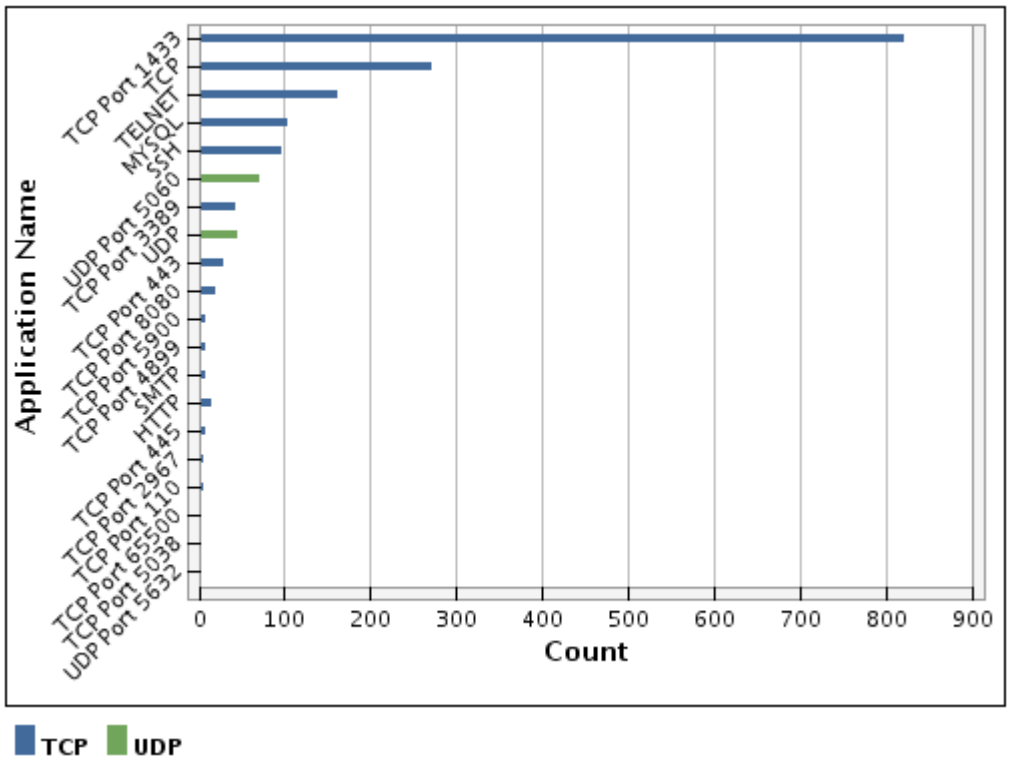
Graph: Top Attacks by Bandwidth

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.



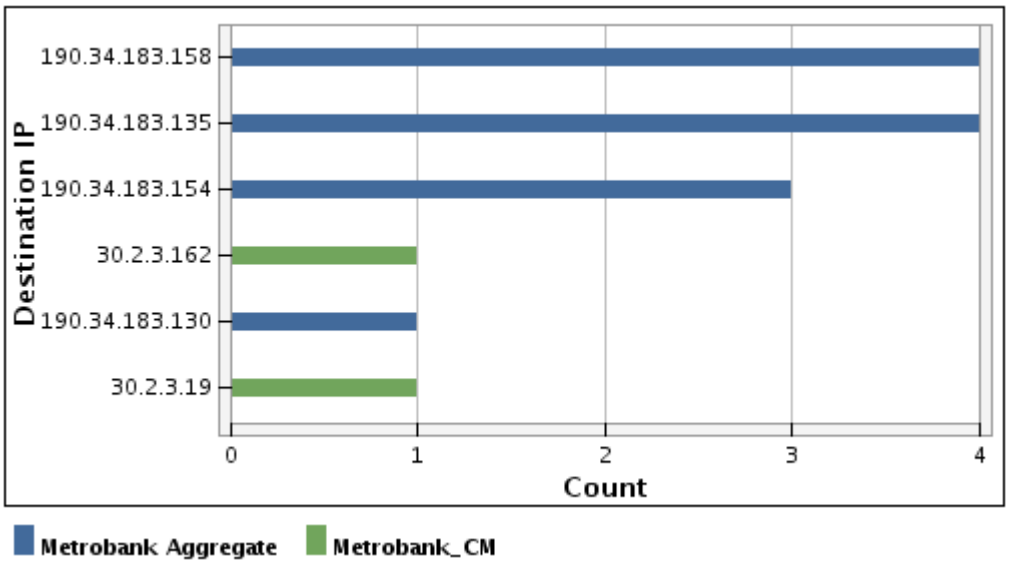
Graph: Top Probed Applications

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.



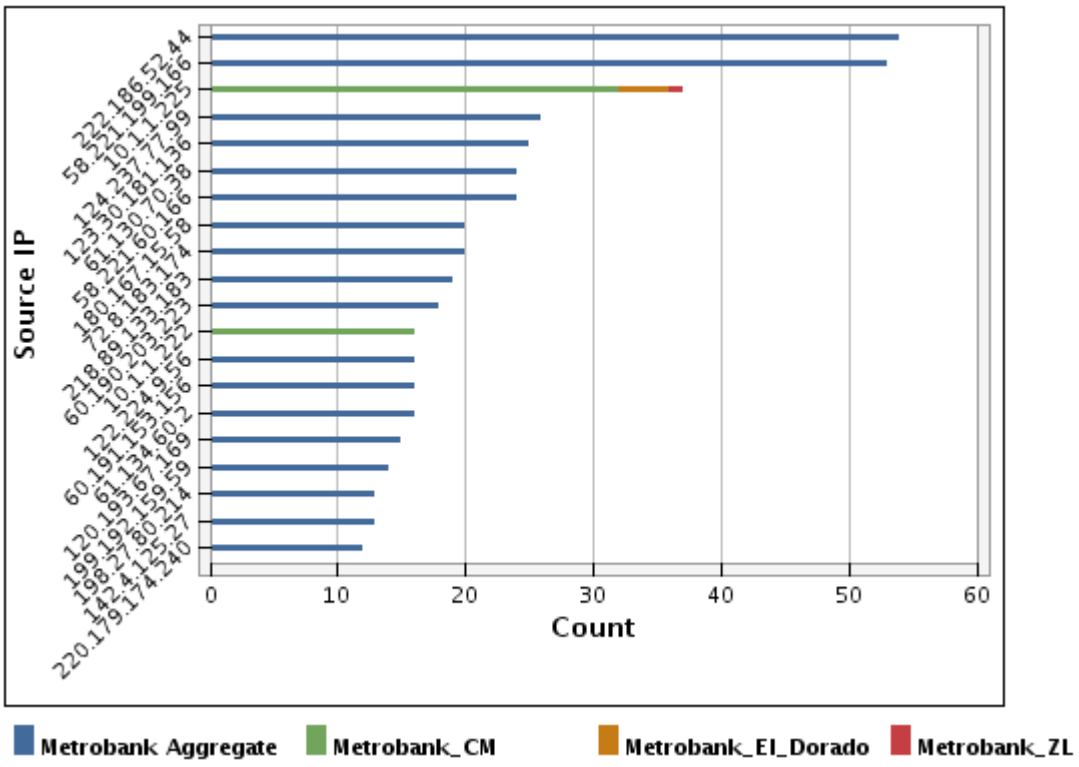
Graph: Top Probed IP Addresses

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 100% of time of time during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	31d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	31d 0h 0m 0s	100.000%	100.000%
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 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
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	99.764% (99.764%)	0.146% (0.146%)	0.000% (0.000%)	0.091% (0.091%)	0.000%
Average	99.764% (99.764%)	0.146% (0.146%)	0.000% (0.000%)	0.091% (0.091%)	0.000%

b) Monitoring system performance

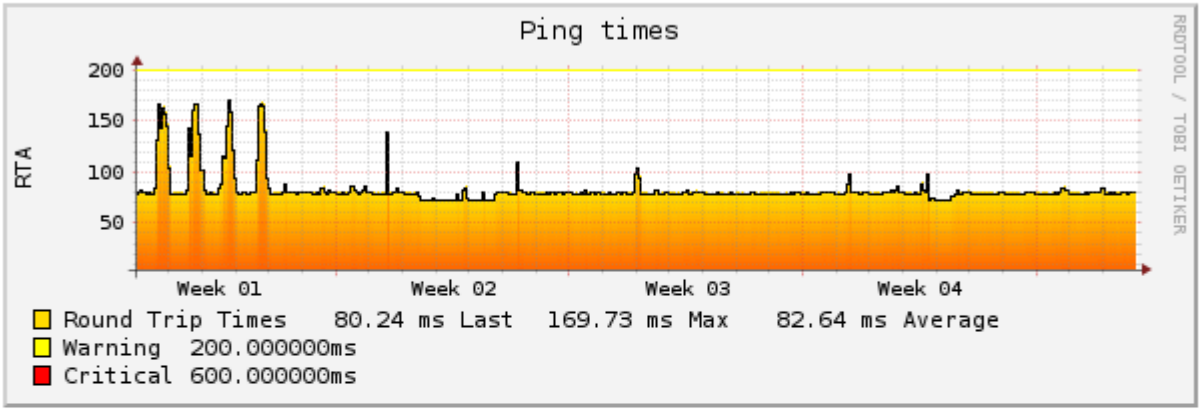
METROBANK DefensePro Ping Performance:

Round trip ping times averaged 82.46 ms from the GLESEC GOC to METROBANK with 0% average packet loss

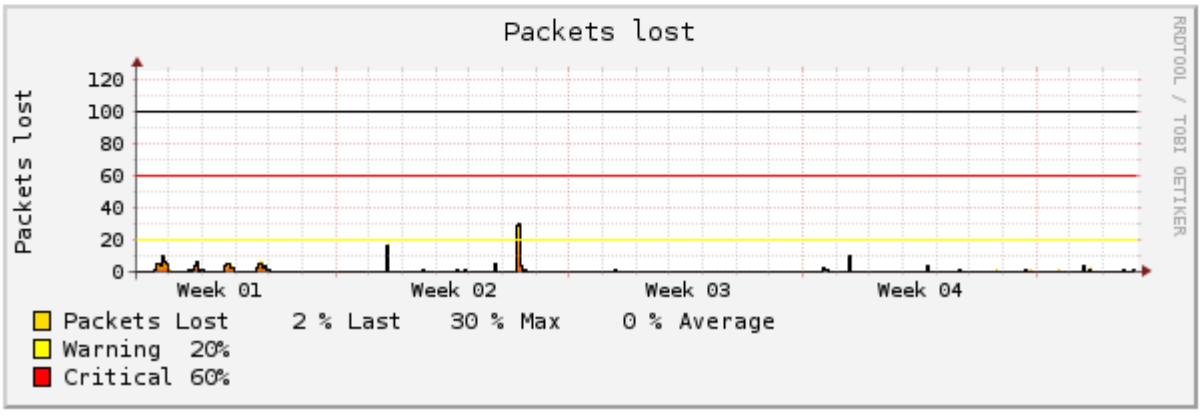
Host: MetroBank DefensePro 508 **Service:** PING

Custom time range 01.01.13 0:00 - 31.01.13 0:00

Datasource: Round Trip Times



Datasource: Packets Lost



METROBANK AppWall Availability:

The AppWall was considered up and available 100% of time of time during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	31d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	31d 0h 0m 0s	100.000%	100.000%
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 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
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	99.787% (99.787%)	0.126% (0.126%)	0.000% (0.000%)	0.087% (0.087%)	0.000%
Average	99.787% (99.787%)	0.126% (0.126%)	0.000% (0.000%)	0.087% (0.087%)	0.000%

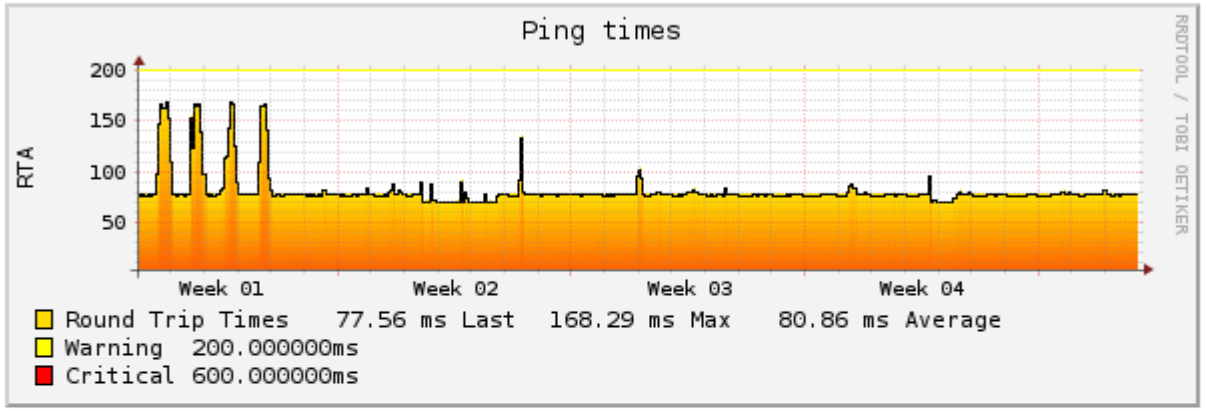
METROBANK AppWall Ping Performance:

Round trip ping times averaged 73.67 ms from the GLESEC GOC to METROBANK with 0% average packet loss

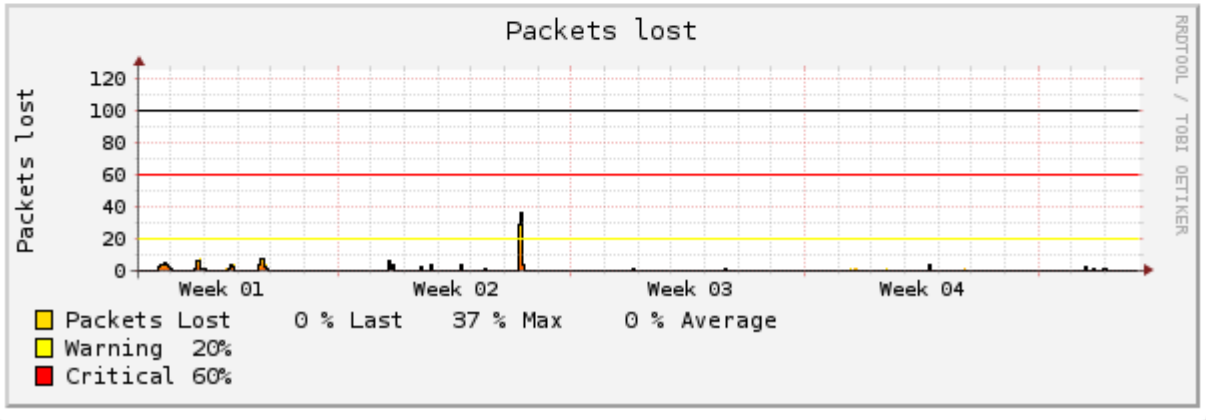
Host: MetroBank AppWall **Service:** PING

Custom time range 01.01.13 0:00 - 31.01.13 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)**

inetnum: 120.192.0.0 - 120.255.255.255
netname: CMNET
descr: China Mobile Communications Corporation
descr: Mobile Communications Network Operator in China
descr: Internet Service Provider in China
country: CN
admin-c: JS686-AP
tech-c: HL1318-AP
status: ALLOCATED PORTABLE
mnt-by: APNIC-HM
mnt-lower: MAINT-CN-CMCC
mnt-routes: MAINT-CN-CMCC
changed: hm-changed@apnic.net 20080414
source: APNIC
route: 120.192.0.0/11
descr: China Mobile communications corporation
origin: AS9808
mnt-by: MAINT-CN-CMCC
changed: lihaijun@chinamobile.com 20081105
source: APNIC
person: Jinxia Sun
address: China Mobile Communications Corporation
address: 29, Jinrong Ave., Xicheng District, Beijing, 100032
country: CN
phone: +86-10-66006688-1755
fax-no: +86-10-66006012
e-mail: sunjinxia@chinamobile.com
nic-hdl: JS686-AP
mnt-by: MAINT-CN-CMCC
changed: hostmaster@chinamobile.com 20030130
source: APNIC
person: haijun li
nic-hdl: HL1318-AP
e-mail: hostmaster@chinamobile.com
address: 29,Jinrong Ave, Xicheng district,beijing,100032
phone: +86 10 66006688
fax-no: +86 10 66006187
country: CN
changed: hostmaster@chinamobile.com 20110824
mnt-by: MAINT-CN-CMCC
source: APNIC

inetnum: 122.224.9.0 - 122.224.9.255
netname: NINBO-LANZHONG-LTD
country: CN
descr: Ninbo Lanzhong Network Ltd
descr:

admin-c: TD231-AP
tech-c: CS64-AP
status: ASSIGNED NON-PORTABLE
changed: auto-dbm@dcb.hz.zj.cn 20100105
mnt-by: MAINT-CN-CHINANET-ZJ-SX
source: APNIC
role: CHINANET-ZJ Shaoxing
address: No.9 Sima Road,Shaoxing,Zhejiang.312000
country: CN
phone: +86-575-5136199
fax-no: +86-575-5114449
e-mail: anti-spam@mail.sxptt.zj.cn
admin-c: CH109-AP
tech-c: CH109-AP
nic-hdl: CS64-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20031204
source: APNIC
changed: hm-changed@apnic.net 20111114
person: Taichun Du
nic-hdl: TD231-AP
e-mail: anti-spam@mail.sxptt.zj.cn
address: Shaoxing,Zhejiang.Postcode:312000
phone: +86-574-88311333
country: CN
changed: auto-dbm@dcb.hz.zj.cn 20100105
mnt-by: MAINT-CN-CHINANET-ZJ-SX
source: APNIC

inetnum: 123.30.0.0 - 123.31.255.255
netname: VDC-NET
country: vn
descr: VietNam Data Communication Company (VDC)
admin-c: VIG1-AP
tech-c: VIG1-AP
status: ALLOCATED NON-PORTABLE
changed: hm-changed@vnnic.net.vn 20090325
mnt-by: MAINT-VN-VNPT
source: APNIC
route: 123.30.128.0/18
descr: VietNam Post and Telecom Corporation (VNPT)
descr: VNPT-AS-AP
country: VN
origin: AS7643
notify: hm-changed@vnnic.net.vn
mnt-by: MAINT-VN-VNPT
changed: hm-changed@vnnic.net.vn 20100121
source: APNIC
role: VDC IPADMIN GROUP
address: Internet Building, Block II, Thang Long Inter Village
address: Nguyen Phong Sac str, Cau Giay Dist, Ha Noi

country: VN
phone: +84-912-800008
fax-no: +84-4-9430427
e-mail: hathm@vdc.com.vn
admin-c: THMH1-AP
tech-c: THMH1-AP
nic-hdl: VIG1-AP
notify: hm-changed@vnnic.net.vn
mnt-by: MAINT-VN-VNPT
changed: hm-changed@vnnic.net.vn 20090325
source: APNIC
changed: hm-changed@apnic.net 20111114

inetnum: 124.237.77.0 - 124.237.77.255
netname: QH-YDZY-ELECTRON-LTD
descr: the yanda zhengyang electron Ltd. of Qinhuangdao
country: CN
admin-c: BR3-AP
tech-c: BR3-AP
status: ASSIGNED NON-PORTABLE
mnt-by: MAINT-CHINANET-HE
changed: renbin@hbtele.com 20090618
source: APNIC
person: Bin Ren
nic-hdl: BR3-AP
e-mail: hostmaster@hbtele.com
address: NO.69 KunLun avenue, Shijiazhuang 050000 China
phone: +86-311-85211771
fax-no: +86-311-85202145
country: CN
changed: renbin@hbtele.com 20060606
mnt-by: MAINT-CHINANET-HE
source: APNIC

NetRange: 142.4.125.0 - 142.4.125.255
CIDR: 142.4.125.0/24
OriginAS: AS54600
NetName: 199-180-100-0-1
NetHandle: NET-142-4-125-0-1
Parent: NET-142-4-96-0-1
NetType: Reassigned
RegDate: 2012-10-25
Updated: 2012-10-25
Ref: http://whois.arin.net/rest/net/NET-142-4-125-0-1
CustName: Anxin
Address: Chengdu
City: Chengdu
StateProv: SICHUAN
PostalCode: 050012
Country: CN
RegDate: 2012-10-25

Updated: 2012-10-25
Ref: http://whois.arin.net/rest/customer/C03192636
OrgAbuseHandle: ABUSE3497-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-657-206-5036
OrgAbuseEmail: abuse@petaexpress.com
OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE3497-ARIN
OrgTechHandle: NOC12550-ARIN
OrgTechName: NOC
OrgTechPhone: +1-657-206-5036
OrgTechEmail: noc@petaexpress.com
OrgTechRef: http://whois.arin.net/rest/poc/NOC12550-ARIN
OrgNOCHandle: NOC12550-ARIN
OrgNOCName: NOC
OrgNOCPhone: +1-657-206-5036
OrgNOCEmail: noc@petaexpress.com
OrgNOCRef: http://whois.arin.net/rest/poc/NOC12550-ARIN

NetRange: 142.4.96.0 - 142.4.127.255
CIDR: 142.4.96.0/19
OriginAS: AS54600
NetName: PT-82-4
NetHandle: NET-142-4-96-0-1
Parent: NET-142-0-0-0-0
NetType: Direct Allocation
RegDate: 2012-07-12
Updated: 2012-07-12
Ref: http://whois.arin.net/rest/net/NET-142-4-96-0-1
OrgName: PEG TECH INC
OrgId: PT-82
Address: 440 North Wolfe Road
City: Sunnyvalle
StateProv: CA
PostalCode: 94085
Country: US
RegDate: 2012-03-27
Updated: 2012-08-03
Ref: http://whois.arin.net/rest/org/PT-82
OrgAbuseHandle: ABUSE3497-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-657-206-5036
OrgAbuseEmail: abuse@petaexpress.com
OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE3497-ARIN
OrgTechHandle: NOC12550-ARIN
OrgTechName: NOC
OrgTechPhone: +1-657-206-5036
OrgTechEmail: noc@petaexpress.com
OrgTechRef: http://whois.arin.net/rest/poc/NOC12550-ARIN
OrgNOCHandle: NOC12550-ARIN
OrgNOCName: NOC
OrgNOCPhone: +1-657-206-5036

OrgNOCEmail: noc@petaexpress.com
OrgNOCRef: http://whois.arin.net/rest/poc/NOC12550-ARIN

inetnum: 180.160.0.0 - 180.175.255.255
netname: CHINANET-SH
descr: CHINANET SHANGHAI PROVINCE NETWORK
descr: China Telecom
descr: No.31,jingrong street
descr: Beijing 100032
admin-c: WWQ4-AP
tech-c: WWQ4-AP
country: CN
status: ALLOCATED PORTABLE
changed: hm-changed@apnic.net 20090821
mnt-by: APNIC-HM
mnt-lower: MAINT-CHINANET-SH
source: APNIC
person: Weng Wen Qian
address: Room 2405,357 Songlin Road,Shanghai 200122
country: CN
phone: +86-21-68405784
fax-no: +86-21-50623458
e-mail: wengwq@online.sh.cn
nic-hdl: WWQ4-AP
mnt-by: MAINT-CHINANET-SH
changed: ip-admin@mail.online.sh.cn 20050403
source: APNIC

NetRange: 198.27.64.0 - 198.27.127.255
CIDR: 198.27.64.0/18
OriginAS: AS16276
NetName: OVH-ARIN-4
NetHandle: NET-198-27-64-0-1
Parent: NET-198-0-0-0-0
NetType: Direct Allocation
RegDate: 2012-08-28
Updated: 2012-08-28
Ref: http://whois.arin.net/rest/net/NET-198-27-64-0-1
OrgName: OVH Hosting, Inc.
OrgId: HO-2
Address: 625, avenue du President Kennedy
Address: Bureau 310
City: Montreal
StateProv: QC
PostalCode: H3A 1K2
Country: CA
RegDate: 2011-06-22
Updated: 2012-04-17
Ref: http://whois.arin.net/rest/org/HO-2
OrgTechHandle: NOC11876-ARIN
OrgTechName: NOC

OrgTechPhone: +33 9 74 53 13 23
OrgTechEmail: noc@ovh.net
OrgTechRef: http://whois.arin.net/rest/poc/NOC11876-ARIN
OrgAbuseHandle: NOC11876-ARIN
OrgAbuseName: NOC
OrgAbusePhone: +33 9 74 53 13 23
OrgAbuseEmail: noc@ovh.net
OrgAbuseRef: http://whois.arin.net/rest/poc/NOC11876-ARIN

NetRange: 199.192.152.0 - 199.192.159.255
CIDR: 199.192.152.0/21
OriginAS: AS53935, AS6939
NetName: VPS21001
NetHandle: NET-199-192-152-0-1
Parent: NET-199-0-0-0-0
NetType: Direct Allocation
RegDate: 2011-08-24
Updated: 2012-03-02
Ref: http://whois.arin.net/rest/net/NET-199-192-152-0-1
OrgName: VPS21 LTD
OrgId: VL-11
Address: 38958 S FREMONT BLVD
City: FREMONT
StateProv: CA
PostalCode: 94536
Country: US
RegDate: 2011-07-26
Updated: 2011-09-24
Ref: http://whois.arin.net/rest/org/VL-11
OrgTechHandle: ZOUJI-ARIN
OrgTechName: zou, jinhe
OrgTechPhone: +1-408-930-0599
OrgTechEmail: zoujinhe@ehostingusa.com
OrgTechRef: http://whois.arin.net/rest/poc/ZOUJI-ARIN
OrgAbuseHandle: ZOUJI-ARIN
OrgAbuseName: zou, jinhe
OrgAbusePhone: +1-408-930-0599
OrgAbuseEmail: zoujinhe@ehostingusa.com
OrgAbuseRef: http://whois.arin.net/rest/poc/ZOUJI-ARIN

inetnum: 218.88.0.0 - 218.89.255.255
netname: CHINANET-SC
descr: CHINANET sichuan province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP
tech-c: XS16-AP
mnt-by: MAINT-CHINANET
mnt-lower: MAINT-CHINANET-SC
status: ALLOCATED NON-PORTABLE

changed: hostmaster@ns.chinanet.cn.net 20020408
changed: hm-changed@apnic.net 20040927
changed: hm-changed@apnic.net 20041126
source: APNIC
person: Chinanet Hostmaster
nic-hdl: CH93-AP
e-mail: anti-spam@ns.chinanet.cn.net
address: No.31 ,jingrong street,beijing
address: 100032
phone: +86-10-58501724
fax-no: +86-10-58501724
country: CN
changed: dingsy@cndata.com 20070416
mnt-by: MAINT-CHINANET
source: APNIC
person: Xiaodong Shi
nic-hdl: XS16-AP
e-mail: ipadmin@my-public.sc.cninfo.net
address: No.72,Wen Miao Qian Str.
address: Data Communication Bureau Of Sichuan Province
address: Chengdu
address: PR China
phone: +86-28-6190785
fax-no: +86-28-6190641
country: CN
changed: ipadmin@my-public.sc.cninfo.net 20030317
mnt-by: MAINT-CHINANET-SC
source: APNIC

inetnum: 220.178.0.0 - 220.180.255.255
netname: CHINANET-AH
country: CN
descr: CHINANET anhui province network
descr: China Telecom
descr: A12,Xin-Jie-Kou-Wai Street
descr: Beijing 100088
admin-c: CH93-AP
tech-c: AT318-AP
status: ALLOCATED non-PORTABLE
changed: wanglinlin2@anhuitelecom.com 20060317
mnt-by: MAINT-CHINANET
source: APNIC
role: ANHUI TELECOM
address: 305 Changjiang West Road
address: Hefei Anhui China
country: CN
phone: +86 0551 5185089
fax-no: +86 0551 5185500
e-mail: wanglinlin2@anhuitelecom.com
admin-c: LW604-AP
tech-c: LW604-AP

nic-hdl: AT318-AP
notify: wanglinlin2@anhuitelecom.com
mnt-by: MAINT-CHINANET-AH
changed: wanglinlin2@anhuitelecom.com 20060323
source: APNIC
changed: hm-changed@apnic.net 20111114
person: Chinanet Hostmaster
nic-hdl: CH93-AP
e-mail: anti-spam@ns.chinanet.cn.net
address: No.31 ,jingrong street,beijing
address: 100032
phone: +86-10-58501724
fax-no: +86-10-58501724
country: CN
changed: dingsy@cndata.com 20070416
mnt-by: MAINT-CHINANET
source: APNIC

inetnum: 222.184.0.0 - 222.191.255.255
netname: CHINANET-JS
descr: CHINANET jiangsu province network
descr: China Telecom
descr: A12,Xin-Jie-Kou-Wai Street
descr: Beijing 100088
country: CN
admin-c: CH93-AP
tech-c: CJ186-AP
mnt-by: APNIC-HM
mnt-lower: MAINT-CHINANET-JS
mnt-routes: MAINT-CHINANET-JS
changed: hm-changed@apnic.net 20040223
status: ALLOCATED PORTABLE
source: APNIC
role: CHINANET JIANGSU
address: 260 Zhongyang Road,Nanjing 210037
country: CN
phone: +86-25-86588231
phone: +86-25-86588745
fax-no: +86-25-86588104
e-mail: ip@jsinfo.net
admin-c: CH360-AP
tech-c: CS306-AP
tech-c: CN142-AP
nic-hdl: CJ186-AP
notify: ip@jsinfo.net
mnt-by: MAINT-CHINANET-JS
changed: dns@jsinfo.net 20090831
changed: ip@jsinfo.net 20090831
changed: hm-changed@apnic.net 20090901
source: APNIC
changed: hm-changed@apnic.net 20111114

person: Chinanet Hostmaster
nic-hdl: CH93-AP
e-mail: anti-spam@ns.chinanet.cn.net
address: No.31 ,jingrong street,beijing
address: 100032
phone: +86-10-58501724
fax-no: +86-10-58501724
country: CN
changed: dingsy@cndata.com 20070416
mnt-by: MAINT-CHINANET
source: APNIC

inetnum: 58.221.199.160 - 58.221.199.175
netname: NANTONG-LANZHOUZHONGHESOFT-CORP
descr: Nantong Lanzhou Zhonghe Soft CORP
descr: Nantong City
descr: Jiangsu Province
country: CN
admin-c: CH448-AP
tech-c: CH448-AP
changed: ip@jsinfo.net 20090602
status: ASSIGNED NON-PORTABLE
mnt-by: MAINT-CHINANET-JS
mnt-lower: MAINT-CHINANET-JS-NT
source: APNIC
person: chinanet-js-nt hostmaster
address: No.88,Huancheng South Road,Nantong 226001
country: CN
phone: +86-513-5518003
fax-no: +86-513-5521614
e-mail: ntip@pub.nt.jsinfo.net
nic-hdl: CH448-AP
mnt-by: MAINT-CHINANET-JS-NT
changed: ip@jsinfo.net 20021211
source: APNIC

inetnum: 58.208.0.0 - 58.223.255.255
netname: CHINANET-JS
descr: CHINANET jiangsu province network
descr: China Telecom
descr: A12,Xin-Jie-Kou-Wai Street
descr: Beijing 100088
country: CN
admin-c: CH93-AP
tech-c: CJ186-AP
mnt-by: APNIC-HM
mnt-lower: MAINT-CHINANET-JS
mnt-routes: MAINT-CHINANET-JS
status: ALLOCATED PORTABLE
changed: hm-changed@apnic.net 20050624
source: APNIC

role: CHINANET JIANGSU
address: 260 Zhongyang Road,Nanjing 210037
country: CN
phone: +86-25-86588231
phone: +86-25-86588745
fax-no: +86-25-86588104
e-mail: ip@jsinfo.net
admin-c: CH360-AP
tech-c: CS306-AP
tech-c: CN142-AP
nic-hdl: CJ186-AP
notify: ip@jsinfo.net
mnt-by: MAINT-CHINANET-JS
changed: dns@jsinfo.net 20090831
changed: ip@jsinfo.net 20090831
changed: hm-changed@apnic.net 20090901
source: APNIC
changed: hm-changed@apnic.net 20111114
person: Chinanet Hostmaster
nic-hdl: CH93-AP
e-mail: anti-spam@ns.chinanet.cn.net
address: No.31 ,jingrong street,beijing
address: 100032
phone: +86-10-58501724
fax-no: +86-10-58501724
country: CN
changed: dingsy@cndata.com 20070416
mnt-by: MAINT-CHINANET
source: APNIC

inetnum: 60.190.203.0 - 60.190.203.255
netname: NINBO-LANZHONG-LTD
country: CN
descr: Ninbo Lanzhong Network Ltd
descr:
admin-c: TD202-AP
tech-c: CS64-AP
status: ASSIGNED NON-PORTABLE
changed: auto-dbm@dcb.hz.zj.cn 20100105
mnt-by: MAINT-CN-CHINANET-ZJ-SX
source: APNIC
role: CHINANET-ZJ Shaoxing
address: No.9 Sima Road,Shaoxing,Zhejiang.312000
country: CN
phone: +86-575-5136199
fax-no: +86-575-5114449
e-mail: anti-spam@mail.sxptt.zj.cn
admin-c: CH109-AP
tech-c: CH109-AP
nic-hdl: CS64-AP
mnt-by: MAINT-CHINANET-ZJ

changed: master@dcb.hz.zj.cn 20031204
source: APNIC
changed: hm-changed@apnic.net 20111114
person: Taichun Du
nic-hdl: TD202-AP
e-mail: anti-spam@mail.sxptt.zj.cn
address: Shaoxing,Zhejiang.Postcode:312000
phone: +86-574-88311333
country: CN
changed: auto-dbm@dcb.hz.zj.cn 20100105
mnt-by: MAINT-CN-CHINANET-ZJ-SX
source: APNIC

inetnum: 60.191.153.152 - 60.191.153.159
netname: WENLING-XINGYU-NETBAR
country: CN
descr: WenLing XingYu Netbar
descr:
admin-c: QZ811-AP
tech-c: CT24-AP
status: ASSIGNED NON-PORTABLE
changed: auto-dbm@dcb.hz.zj.cn 20100513
mnt-by: MAINT-CN-CHINANET-ZJ-TZ
source: APNIC
role: CHINANET-ZJ Taizhou
address: No.668 Shifu Street,Jiaojiang,Taizhou,Zhejiang.318000
country: CN
phone: +86-576-8680619
fax-no: +86-576-8680613
e-mail: anti-spam@mail.tzptt.zj.cn
admin-c: CH111-AP
tech-c: CH111-AP
nic-hdl: CT24-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20031204
source: APNIC
changed: hm-changed@apnic.net 20111114
person: QingQin Zhu
nic-hdl: QZ811-AP
e-mail: anti-spam@mail.tzptt.zj.cn
address: Youdianyu, Zheguo,Wenling,Zhejiang.Postcode:317500
phone: +86-576-86440107
country: CN
changed: auto-dbm@dcb.hz.zj.cn 20100513
mnt-by: MAINT-CN-CHINANET-ZJ-TZ
source: APNIC

inetnum: 61.130.70.36 - 61.130.70.39
netname: DIAN-JIAO-ZHONG-XIN
country: CN
descr: longyouxiandianjiaozhongxin

descr:
admin-c: HQ284-AP
tech-c: CQ11-AP
status: ASSIGNED NON-PORTABLE
changed: auto-dbm@dcb.hz.zj.cn 20071227
mnt-by: MAINT-CN-CHINANET-ZJ-QZ
source: APNIC
role: CHINANET-ZJ Quzhou
address: No.1 Jiangbin Road(North),Quzhou,Zhejiang.324000
country: CN
phone: +86-570-3047163
fax-no: +86-570-3049169
e-mail: anti-spam@mail.qzptt.zj.cn
admin-c: CH106-AP
tech-c: CH106-AP
nic-hdl: CQ11-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20031204
source: APNIC
changed: hm-changed@apnic.net 20111114
person: hu qinghong
nic-hdl: HQ284-AP
e-mail: zj_telecom@zjtelecom.cn
address: Longyou,Quzhou,Zhejiang.Postcode:324400
phone: +86-570-7015522
country: CN
changed: auto-dbm@dcb.hz.zj.cn 20071227
mnt-by: MAINT-CN-CHINANET-ZJ-QZ
source: APNIC

inetnum: 61.134.0.0 - 61.134.63.255
netname: CHINANET-SN
descr: CHINANET Shanxi(SN) province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP
tech-c: XC9-AP
mnt-by: MAINT-CHINANET
mnt-lower: MAINT-CHINANET-SHAANXI
status: ASSIGNED NON-PORTABLE
changed: hostmaster@ns.chinanet.cn.net 20000601
changed: hm-changed@apnic.net 20040927
source: APNIC
person: Chinanet Hostmaster
nic-hdl: CH93-AP
e-mail: anti-spam@ns.chinanet.cn.net
address: No.31 ,jingrong street,beijing
address: 100032
phone: +86-10-58501724
fax-no: +86-10-58501724

country: CN
changed: dingsy@cndata.com 20070416
mnt-by: MAINT-CHINANET
source: APNIC
person: Xianghong Cao
address: Shanxi provice data communication Bureau
address: Xi'an city, Shanxi provice 710061
country: CN
phone: +8629-523-3633
fax-no: +8629-522-8093
e-mail: sxic@public.xa.sn.cn
nic-hdl: XC9-AP
mnt-by: MAINT-NULL
changed: caoxianghong@263.net 19990409
source: APNIC

NetRange: 72.8.128.0 - 72.8.191.255
CIDR: 72.8.128.0/18
OriginAS: AS25761
NetName: STAMINUS-COMMUNICATIONS
NetHandle: NET-72-8-128-0-1
Parent: NET-72-0-0-0-0
NetType: Direct Allocation
RegDate: 2006-09-14
Updated: 2012-03-02
Ref: http://whois.arin.net/rest/net/NET-72-8-128-0-1
OrgName: Staminus Communications
OrgId: STAMIN-2
Address: 502 S. Harbor Blvd.
City: Fullerton
StateProv: CA
PostalCode: 92832
Country: US
RegDate: 2002-05-02
Updated: 2012-05-15
Ref: http://whois.arin.net/rest/org/STAMIN-2
ReferralServer: rwhois://rwhois.staminus.net:4321
OrgTechHandle: TECH380-ARIN
OrgTechName: TECH
OrgTechPhone: +1-949-202-5305
OrgTechEmail: support@staminus.net
OrgTechRef: http://whois.arin.net/rest/poc/TECH380-ARIN
OrgNOCHandle: NOC11206-ARIN
OrgNOCName: NOC
OrgNOCPhone: +1-949-202-5305
OrgNOCEmail: support@staminus.net
OrgNOCRef: http://whois.arin.net/rest/poc/NOC11206-ARIN
OrgAbuseHandle: ABUSE2456-ARIN
OrgAbuseName: ABUSE
OrgAbusePhone: +1-949-202-5305
OrgAbuseEmail: abuse@staminus.net

OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE2456-ARIN
Found a referral to rwhois.staminus.net:4321.