Guest Access to the Internet

Techniques for maintaining highly secured networks

Document Author: Michael A Hawkins Last Edited: October 31st 2017

Introduction

Guest access to the Internet is a common configuration and requirement in enterprise networks large and small. A common method for delivery of guest Internet access is to provide access to all protocols and all services. However, this broad approach may not be wise because it does not provide adequate protection against certain security and operational threats. This document discusses some of the methods that can be used to control guest access to the Internet. While this document provides some guidance, it is not intended to be "the" solution for any specific organization but is rather a point of reference that can be used to begin considering guest access in alternative ways that account for some of those security risks.

Disclaimer for Errors and Omissions: Every reasonable effort has been made to ensure the accuracy, validity and usefulness of the information provided in this assessment report. However, as policies, dates, conditions, best practices, certifications, regulations and information are continually changing, we reserve the right to change at any time and without notice, any information contained herein and make no warranties or representations as to its accuracy or usefulness for any purpose whatsoever.

Table of Contents

Guest Access to the Internet

Guest access to the Internet is a common configuration and requirement in enterprise networks large and small. A common method for delivery of guest Internet access is to provide access to all protocols and services. However, firewall policy management products and tools (such as Algosec, Skybox, Tufin, Firemon etc) flag certain risks based upon 'Any' found in source, destination or service columns. A common risk that will be detected will be open outgoing access to the Internet from guest networks. A guest network is commonly partitioned off from all other parts of the network (using layer 2 VLAN's and or layer 3 routing controls) and firewall rules are configured to allow the guess network/s to reach the Internet and only the Internet. Guest networks are usually denied access to any network within the client organization. Only the Internet can be reached. Other than that network restriction, it is very common to see guest networks configured with no other controls in place. It is often the case that there will be no restrictions on which application protocols the guest network uses to reach the Internet.

Guest access to any Internet protocol or service port is sub-optimal because:

1. There are known protocols that are rarely used for anything but nefarious purposes.
2. There are known protocols that are used specifically for data leakage (exfiltration). And although a guest network is intended to provide unrestricted access to the Internet, there are reasonable restrictions that can and should be implemented to reduce the risk of data leakage.
3. Guest networks should not be so open that they can be used as the source of DoS attacks. Nor should they be configured so that devices that are attached can be easily controlled as part of

a botnet. Nor should the open access be such that known risky protocols may be used when they can be blocked very easily without interfering with the vast majority of guest Internet access requirements.

4. Some application protocols are bandwidth hogs and have a strong potential to interfere with guest Internet services. And if the same infrastructure that supports the organization network also supports the guest network, then there is a reasonable likelihood that such bandwidth hogs might interfere with the organization network too.

5. Access to peer to peer file sharing services can present an organization with legal risks and penalties.

Advanced Features

The guidelines do not address or discuss other advanced features such as user authenticated traffic access rules, URL filtering and layer 4 and above application inspection and control features. Nor does this document discuss anti-malware, anti-virus and other features found in more firewall models (especially so-called 'nex-gen' firewalls). This is not to suggest that these features should not be used. To the contrary, if they are available, they should be used and combined with the techniques described in this document.

Why use “Block and Allow”?

A question often arises as to why it is appropriate to use a series of block (deny) rules followed by allow (permit) rules. It is often very useful to be able to quickly identify and remove a guest device that is attempting to use any of the blocked services. This is especially true if the device is causing problems on the guest network (bandwidth or nefarious etc) that causes an investigation to be launched that requires the examination of the firewall logs.

Block Microsoft Services

Microsoft services should be explicitly blocked in general and guest access to the Internet is no exception. See the document “Firewall Policy Best Practices - Blocking Microsoft NETBIOS” for additional detail regarding blocking Microsoft services.

Block Small Services

The following services can be used for DoS attacks and serve almost no useful purpose for guest networks. They should be blocked.

Service Name	Protocol	Port Number	Notes

echo	TCP, UDP	7	Character echo
chargen	TCP, UDP	19	Character generator
Discard	TCP, UDP	9	Character black hole
Daytime	TCP	19	Returns date and time (superseded by NTP and other time protocols)

Create service objects for each of the small services (both TCP and UDP where appropriate) and add the services to a group named 'Small-Services' or add the services to the group object discussed below.

Block Rare Protocols

Various protocols exist that are not intended for user activities or are rarely used on the Internet. Block these protocols unless they are known to be required. The list is by no means exhaustive or complete and additional protocols can and should be added to the list and should be included in the blocking group object. Some protocols in the list below are marked as optional and may be included or excluded as desired.

A group object should be created that include the list of protocol services below. Multiple groups can be created to be applied to specific guest groups. For guest access to the Internet, a suitable group name might be **"Guest -Block -Risky-Services"**.

Service Name	Protocol	Port	Notes
bgp	TCP	179	
cifs	TCP, UDP	3020	
Citrix-ica	TCP	1494	Optional
ctiqbe	TCP	2748	
exec	TCP	512	
finger	TCP	79	
gopher	TCP	70	
h323	TCP	1720	
hostname	TCP	101	

ident	TCP	113	
klogin	TCP	543	
kshell	TCP	544	
ldap	TCP	389	
ldaps	TCP	636	
login	TCP	513	
lotusnotes	TCP	1352	
lpd	TCP	515	
mssql	TCP, UDP	1433, 1434	
mysql	TCP, UDP	3306	
nfs	TCP, UDP	2049	
nntp	TCP	119	Optional*
oracle	TCP	1521, 1522, 1525, 1529	
pcanywhere	TCP	5631	
pop2	TCP	109	
rsh	TCP	514	
rtsp	TCP	554	
sip	TCP, UDP	5060	Optional*
sqlnet	TCP	1521	
sunrpc	TCP	111	
tacacs	TCP	49	
talk	TCP	517	
telnet	TCP	23	
teredo	UDP	3544	IPv6 tunneling behind IPv4 NAT
biff	UDP	512	
bootpc	UDP	68	

bootps	UDP	67	
cifs	UDP	3020	
dnsix	UDP	195	
kerberos	UDP	750	
mobile	UDP	432	
nameserver	UDP	42	
ntp	UDP	123	Optional*
pcanywhere	UDP	5632	Optional*
pim-auto-rp	UDP	436	
radius	UDP	1645, 1812	
radius-acct	UDP	1646, 1813	
rip	UDP	520	
secureid	UDP	5510	
snmp, snmptrap	UDP	161, 162	
sunrpc	UDP	111	
syslog	UDP	514	
tacacs	UDP	49	
talk	UDP	517	
tftp	UDP	69	
time	UDP	37	
who	UDP	513	
xdmcp	UDP	177	

Note*: optional protocols may be permitted dependent upon client requirements for guests.

Blocking Peer to Peer File Sharing Services

The most common file share services are listed below.

Service Name	Protocol	Port	Notes

BitTorrent	TCP	6881-6999	Also Azureus
Blubster	UDP	41170	
Direct_connect	TCP, UDP	411,412	
eDonkey	TCP, UDP	4661,4662,4665	
GNUtella	TCP, UDP	6346,6347	Also Limewire
Hotline	TCP, UDP	5500-5503, 5499	
iMesh	TCP	5000	
KaZaa	TCP	1214	
Madster	TCP	5025	
Napster	TCP	6600-6699, 4444, 5555, 6666, 7777, 8888, 8875	
WinMX	TCP, UDP	6699, 6257	

The list above is by no means exhaustive or complete and additional protocols can and should be added to the list and should be included in the P2P file sharing group. Checkpoint has a group already defined that includes most (but not all) of the above services. You may wish to add those that are missing and also do an Internet search to find more.

Blocking Trojan Services

The list of backdoor service ports that are used by Trojans is very long. ***Checkpoint has a preexisting group named Trojan_Services*** that can be used to block Trojan traffic access sourcing from guest networks.

Blocking Online Gaming Services

Game Name	Protocols	Service Port	Notes
GTA2	TCP, UDP	2300 to 2400, 47624	Multiplayer game.
Half Life 2	TCP, UDP	1200, 27000 to 27015, 27020 to 27039	Multiplayer game.
Age of Empires	TCP, UDP	2300 to 2400, 6073, 47624	Multiplayer game.

Call of Duty	TCP, UDP	20500, 20510, 28960	Multiplayer game.
Counter-Strike	TCP, UDP	1200, 27000 to 27015, 27020 to 27039	Multiplayer game.
Doom 3	TCP, UDP	27650, 27666	Multiplayer game.
Everquest	TCP, UDP	1024, 6000, 7000	Multiplayer game.
Far Cry	TCP, UDP	49001 to 49002, 49124	Multiplayer game.
FIFA	TCP, UDP	3658, 10400 to 10499	Multiplayer game.
Microsoft Flight Simulator	TCP, UDP	2300 to 2400, 6073, 23456, 47624	Multiplayer game.
Gamespy Arcade	TCP, UDP	3783, 6515, 6500, 6667, 13139, 27900, 28900, 29900, 29901	Game browser.
NBA Live	UDP	3658, 9570, 18699 to 28600	Multiplayer game.
Need For Speed	TCP, UDP	80, 1030, 3658, 3659, 9442, 13505, 18210, 18215, 30900 to 30999	Multiplayer game.
Neverwinter Nights	UDP	5120 to 5300, 6500, 6667, 27900, 28900	Multiplayer game.
NHL	TCP, UDP	3658, 10300, 13505	Multiplayer game.
No One Lives Forever	TCP, UDP	2300 to 2400, 7000 to 10000, 27888	Multiplayer game.
Quake	TCP, UDP	27650, 27910, 27950, 27952, 27960, 27965	Multiplayer game.
Rainbow Six	TCP, UDP	80, 2346 to 2348, 6667, 7777 to 7787, 8777 to 8787, 40000 to 42999, 44000, 45000	Multiplayer game.
Soldier of Fortune	TCP, UDP	28910 to 28915, 20100 to 20112	Multiplayer game.
Starcraft	TCP, UDP	6112	Multiplayer game.
Tiger Woods PGA Tour	TCP, UDP	80, 443, 9570, 13505, 20803, 20809, 32768 to 65535	Multiplayer game.

Tribes	TCP, UDP	28000, 28001	Multiplayer game.
Ultima Online	TCP	5001 to 5010, 7775 to 7777, 7875, 8800 to 8900, 9999	Multiplayer game.
Unreal Tournament	TCP, UDP	7777 to 7788, 8080, 8777, 9777, 27900, 42292	Multiplayer game.
Warcraft	TCP, UDP	6112 to 6119	Multiplayer game.
World of Warcraft	TCP	3724, 6112, 6881 to 6999	Multiplayer game.
Worms Armageddon	TCP	80, 6667, 17010 to 17012	Multiplayer game.
XBox	TCP, UDP	80, 1900, 3390, 3074, 3776, 3932, 5555, 7777	Game appliance.

Note*: port 80 and 443 are included above for clarity. However, blocking of those ports cannot be done unless network destinations are determined and rules created for each specific game. Instead, it is possible to block all other ports for each game. Blocking the non-standard ports is generally sufficient to stop gaming from occurring from the guest network.

VPN Client Services

Access to VPN client services is a relatively common requirement so an additional rule may be necessary to permit client VPN services.

SSH/SFTP and FTP Services

Access to SSH (and thus SFTP) or FTP file transfer services is a common requirement so an additional rule may be necessary to permit SSH and or FTP. However, we recommend avoiding providing access to these two services if possible as they both present a risk of data leakage.

Allowing Guest Access to the Internet

So far, we have been discussing the services that might be blocked in order to protect your organization from legal action (as for illegal file sharing activities), bandwidth hogging (as for gaming applications and music streaming) and leaking of data (either intentional or accidental). Now we must put together our recommended solution that it also takes into account standard best practices including:

1. Not mixing functions/purposes within single rules.
2. Not mixing un-encrypted and encrypted services within single rules.

Services that are commonly provided and are expected to function on a guest network are:

1. Web browsing (both http and https).
2. Mail services.
3. Instant messaging services.
4. Optional: VPN client protocols, file transfer (FTP) and secured file transfer (SFTP/SSH).

Taking into consideration all of the above sections and points we arrive at the following recommendation for the end state. Note that the drop rules may initially be set to permit for some period of time in order to avoid any unexpected interruptions to guest access operations. But the long term goal is to block as much as possible while allowing the access that is actually necessary:

	- Guest Internet Access (Rules 15-24)							
15	0	block Microsoft NETBIOS	GUEST_WIRELESS	The_Internet	Any	Microsoft-NETBIOS	drop	Log
16	0	block risky services	GUEST_WIRELESS	The_Internet	Any	Guest-Block-Risky-Services	drop	Log
17	0	block P2P file sharing	GUEST_WIRELESS	The_Internet	Any	P2P_File_Sharing_Applicatio	drop	Log
18	0	block trojans	GUEST_WIRELESS	The_Internet	Any	Trojan_Services	drop	Log
19	0	block gaming	GUEST_WIRELESS	The_Internet	Any	Guest_Block_Gaming	drop	Log
20	0	allow HTTP	GUEST_WIRELESS	The_Internet	Any	http	accept	Log
21	0	allow HTTPS	GUEST_WIRELESS	The_Internet	Any	https	accept	Log
22	0	allow IM	GUEST_WIRELESS	The_Internet	Any	Messenger_Applications	accept	Log
23	0	allow unencrypted email	GUEST_WIRELESS	The_Internet	Any	Mail_Unencrypted	accept	Log
24	0	allow encrypted mail	GUEST_WIRELESS	The_Internet	Any	Mail_Encrypted	accept	Log

Finally, if the above restrictions and permissions must be introduced in such a way as to not interfere with existing guest access then the following catch all can be added as the very last rule and hits on the rule can be monitored and investigated so that additional services can be provisioned if necessary. In this manner, additional blocking or permitting can be introduced over time until it is appropriate to remove the general 'any' services rule.

25	0	allow everything else	GUEST_WIRELESS	The_Internet	Any	Any	accept	Log

It is our recommendation that the above rule be treated as temporary and that when a sufficient time has passed and no activity is seen (or any activity is investigated to your satisfaction) that the rule should be disabled and then deleted.

Other Services

Various other services can and do interfere with the delivery of reliable services on guest networks. The list below covers some of the more common media services that can consume bandwidth. Additional services group and rules may be provisioned to handle other services as needed.

Application	Protocol	Ports	Notes
iTunes	TCP, UDP	3689	Music sharing application.
Net2Phone	UDP	6801	VoIP application.
NetFone	TCP	10200	VoIP application.
PhoneFree	TCP, UDP	1034 to 1035, 2644, 8000, 9900 to 9901	VoIP application.
Quicktime	TCP, UDP	6970 to 7000	Video streaming application.
Speak Freely	UDP	2074 to 2076	VoIP application.
TeamSpeak	TCP, UDP	8767, 14534, 51234	Online voice chat.
Winamp Streaming	TCP	8000 to 8001	Audio streaming application.
WebcamXP	TCP	8080, 8090	Video sharing application.

Where to Next?

For additional information regarding firewall policy traffic rules best practices, guidelines and technical details, see https://www.wantegrity.com/firewall-policy-management-collateral/

<END>