Report for:

FortiGate Firewall Review Sample Report

ClientName

May 18, 2021

Version: 3.0

Prepared by: NCC Consultant

Email: n.consultant@nccgroup.com

Telephone: +44 (0)161 209 5200

NCC Group PLC - Security Testing Audit and Compliance

XYZ Building,
2 Hardman Boulevard,
Spinningfields,
Manchester,
M3 3AQ
https://www.nccgroup.com

1 Executive Summary

This report presents the findings of the FortiGate Firewall Review security assessment conducted on behalf of Client Company Ltd (ClientName). The assessment was conducted on 14/05/2021 and was authorised by ClientName.

The system being assessed was a FortiGate firewall used to provide internal network segregation.

1.1 Overview

The Firewall Review identified one high risk issue which could allow a user to bypass a requirement to use a second authentication factor. That is, they would not need to supply an extra token in addition to the correct password and so this would increase the risk of unauthorised access. Other issues could allow an attacker to disrupt the network and so affect the availability of internal systems. Risk was primarily exposed because of the use of outdated software with known vulnerabilities. Other, lower risk, issues were the result of deviations from security best practice in the device configuration.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
Phase 1 –Firewall Configuration Review	0	1	2	9	**12**
Total	**0**	**1**	**2**	**9**	**12**

1.2 Assessment Summary

It was noted that the version of the operating system in use by the firewall was outdated and so was vulnerable to known security issues. A weakness in the authentication mechanism could be exploited so as to allow someone in possession of a valid set of credentials to bypass any requirement to supply a second authentication factor. That is, they would not need to supply an extra token in addition to the correct password even though this was supposedly required. This would increase the risk of unauthorised access. In addition, an attacker could recover information about the firewall platform (such as model and version information) and this information could be recovered without any need to authenticate. It is acknowledged that an attacker would need to be located within the relevant network segment to access a device; nevertheless, as the unpatched issues included an authentication flaw, this finding was assessed to pose a high risk. The continued use of this version may be indicative of a gap in the software patching procedures.

The review of the firewall ruleset itself identified rules which were not appropriately restrictive. Users might be able to access services for which there was no clear business requirement. Rules were present which did not sufficiently restrict either the source or destination addresses or, in a number of cases, which service was permitted.

In addition, a rule was present which permitted connections to two hosts over a legacy management protocol that does not use encryption. A suitably placed attacker could therefore be able to capture this management traffic, leading to them gaining administrative access to those devices.

Beyond this, a number of issues are raised relating to security best practice, the resolution of which would further increase the device's security posture. It is important to recognise that even low risk issues can often be exploited in combination with higher risk issues as part of a wider attack which seeks to compromise an environment or application.

More detailed information on each of the issues which were identified is included in the Technical Details.

1.3 Strategic Recommendations

The firewall operating system was found to be outdated. This should be updated to the latest stable and secure version. In addition, the use of outdated software on this important network device may be an indication that the organisation’s patching policies and procedures would benefit from review. In general, these procedures should cover all the devices and technology in use across the information estate. However, it is particularly important that network switches, filtering devices and any perimeter devices should be kept up-to-date. The exploitation of known vulnerabilities exposed through the use of outdated software on devices of this type could have a considerable impact.

The firewall rules were not appropriately restrictive. As firewalls are designed to be a security barrier, rules should be as restrictive as is consistent with maintaining the functionality required by the business. It is recommended that a review is undertaken to rationalise the ruleset with a view to minimising the access they provide.

An unencrypted protocol was in use. Support for unencrypted protocols should be withdrawn in favour of robustly encrypted alternatives and the ruleset amended in support of these alternatives.

2 Table of Contents

1 Executive Summary 2
1.1 Overview 2
1.2 Assessment Summary 2
1.3 Strategic Recommendations 3
2 Table of Contents 4
3 Technical Summary 5
3.1 Scope 5
3.2 Caveats 5
3.3 Post Assessment Cleanup 5
3.4 Risk Ratings 6
3.5 Findings Overview 7
4 Technical Details 9
4.1 Phase 1 –Firewall Configuration Review 9
5 Supplemental Data - Widely Scoped ACLs 28
6 Supplemental Data - Test / Temporary Rules 29
7 Document Control 31
7.1 Document Data 31
7.2 Document History 31
7.3 Document Distribution List 31
8 Assessment Team 32

3 Technical Summary

NCC Group was contracted by ClientName to conduct a security assessment of the FortiGate firewall cluster in order to identify security issues that could negatively affect ClientName's business or reputation if they led to the compromise or abuse of systems.

3.1 Scope

The security assessment was carried out in the production environment and involved the following section of work:

- Firewall Configuration Review

The following device was within the scope of this test:

- FORTIFW01

3.2 Caveats

The scope of work defined two devices; however, as these firewalls were configured to operate within an active-active cluster it was deemed appropriate to review just one device configuration.

3.3 Post Assessment Cleanup

Any test accounts which were created for the purpose of this assessment should be disabled or removed, as appropriate, together with any associated content.

Revert any WAF/IDS/IPS/firewall changes which were made for the purposes of the assessment.

3.4 Risk Ratings

The table below gives a key to the icons and symbols used throughout this report to provide a clear and concise risk scoring system. It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

Symbol	Risk Rating	CVSSv2 Score	Explanation
✖	CRITICAL	9.0 - 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.
⛔	HIGH	7.0 - 8.9	A vulnerability was discovered that has been rated as high. This requires resolution in the short term.
!	MEDIUM	4.0 - 6.9	A vulnerability was discovered that has been rated as medium. This should be resolved as part of the ongoing security maintenance of the system.
△	LOW	1.0 - 3.9	A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks.
i	INFO	0 - 0.9	A discovery was made that is reported for information. This should be addressed in order to meet leading practice.
✓	GOOD	N/A	Good security practices were being followed or an audit item was found to be present and correct.

3.5 Findings Overview

All the issues identified during the assessment are listed below with a risk rating for each issue.

Phase 1 –Firewall Configuration Review

Ref	Finding	Risk
SR-104-001	**Device Software Vulnerabilities**	High ⛔
SR-104-002	**Widely Scoped Access Controls**	Medium ❗
SR-104-003	**Rule Permits a Legacy Clear Text Protocol**	Medium ❗
SR-104-004	**Test / Temporary Rules Present**	Low △
SR-104-005	**Rules Allow Any ICMP Message Type**	Low △
SR-104-006	**Proxy Address Resolution Protocol (ARP) was Enabled**	Low △
SR-104-007	**ICMP Redirect Messages Were Enabled**	Low △
SR-104-008	**Network Time Source Not Authenticated**	Low △
SR-104-009	**Unrestricted Administrative Interfaces**	Low △
SR-104-010	**No Pre-Logon Banner Message**	Low △
SR-104-011	**Local Based Authentication**	Low △
SR-104-012	**Duplicate / Overlapping Rules**	Low △

Ref	Finding	Risk
SR-104-013	**Disabled Rules Present**	Info ℹ
SR-104-014	**Rules without Comment Text or Annotation**	Info ℹ

4 Technical Details

4.1 Phase 1 –Firewall Configuration Review

SR-104-001	Device Software Vulnerabilities		⛔
Risk Rating	High	**Status**	Open

Description:

The firewall was running an outdated version of the FortiOS operating system software. This was identified as version 6.2.3, released in December 2019. At the time of writing, the latest stable and supported version in this branch was 6.2.8, released in April 2021. The installed version of the software contained an authentication flaw which could allow someone in possession of a valid set of user credentials to bypass the requirement for a second factor of authentication.

In addition, there was an information disclosure vulnerability which could allow a remote attacker to recover information about the platform including version and model information. This issue was originally addressed in version 6.2.1 but was re-introduced in version 6.2.3.

The software version from the device configuration was checked against the FortiOS release notes; this showed that it contained the vulnerabilities below:

CVE Reference	CVSSv2	Fixed in Version
CVE-2018-13367	5.0	6.2.4, 6.4.0
CVE-2020-12812	9.8	6.2.4, 6.4.0

It is extremely important that software is regularly maintained with patches and upgrades in order to help mitigate the risk of an attacker exploiting a known software vulnerability. In addition to security features and fixes, software updates will often include additional functionality, performance improvements and features.

Recommendation:

The latest system software upgrades, updates or patches should be applied within a short time following their release by the vendor. Additionally, it is suggested that the current patching policy should be reviewed to ensure that future updates are applied in a timely manner.[1]

In addition the length of time this software has remained outdated suggests that this software is outside the software patching process. The reason for this should be identified and addressed.

Affects:

Device	Installed	Latest
FORTIFW01	6.2.3	6.2.8, 6.4.5

[1] **FortiOS Release Notes** https://docs.fortinet.com/document/fortigate/6.2.8/fortios-release-notes/760203/introduction-and-supported-models

SR-104-002	Widely Scoped Access Controls		!
Risk Rating	Medium	**Status**	Open

Description:

Rules were observed that could be considered overly permissive and allow potentially inappropriate traffic flows. A weak configuration could contribute to a malicious user or an attacker gaining unauthorised access to network services.

The primary purpose of a firewall is to be a security barrier, preventing unauthorised access to devices and services by filtering the network traffic. The network filtering can be configured to allow or deny access from specific network addresses to specific network addresses and specific services. Best practice dictates that access to services should only be configured for those hosts that require it and that this should be restricted on a need-only basis to the required services.

The potential risk from this issue is that an attacker could leverage these widely scoped rules to communicate with hosts or network subnets which they should not be able to. In the event of a compromise of any server it is important that the firewall restricts the accessibility an attacker has.

Full details of rules considered overly permissive are detailed in Supplemental Data - Test / Temporary Rules on page 29.

Recommendation:

In general, network filtering rules should be as restrictive as possible while still maintaining business functionality. Rules should be configured to restrict access to network addresses and services from only those hosts that require it. Devices provided for a specific service should allow access only to that service and should not use the 'Any' keyword.

Rules should be modified where feasible, to restrict the traffic to specific hosts and services as required. The following best practice guidelines should be followed:

- rules do not allow access from any source
- rules do not allow access to any port from a source network address
- rules do not allow access to any destination
- rules do not allow access to any port on a destination network address
- rules do not allow access to any destination service
- rules do not allow access to a range of destination services

However, it is worth noting that it may not be possible to achieve this in all circumstances, such as with a public web server where business requirements imply that any network address should be permitted to access the service.

Affects:

Device
FORTIFW01

SR-104-003	Rule Permits a Legacy Clear Text Protocol		!
Risk Rating	Medium	**Status**	Open

Description:

A single firewall rule permitted access via the legacy clear text protocol, Telnet. Information that travels along a Telnet connection is not encrypted, as such data including credentials are susceptible to interception.

Due to the lack of encryption provided by the Telnet protocol, an attacker who is able to monitor a Telnet session would be able to view all of the authentication credentials and data passed in the session. The attacker could then attempt to gain access to the device using the authentication credentials extracted from

The associated rule from the Production VDOM is presented below:

Rule	Action	Source	Destination	Service
139	Allow	PSZ_RDS_10.107.143.0/26	switch01.uk.acme.com_10.171.186.81 switch02.uk.acme.com_10.171.186.82	TELNET

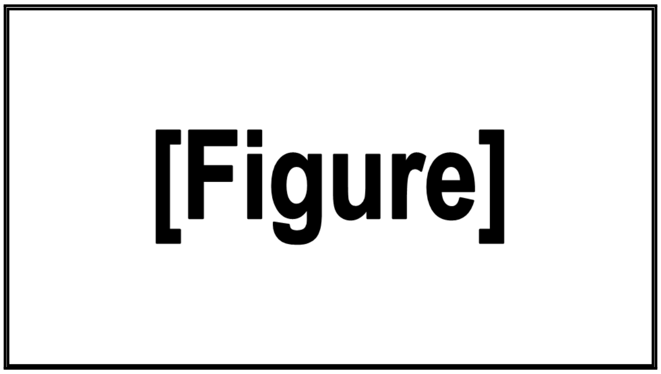

Figure 1: SECUREZONE-LIVE-INF to ZONE1-LIVE

Recommendation:

Where possible, the use of clear text protocols should be avoided. The network services associated with the identified rule should be decommissioned and replaced with cryptographically secure alternatives. Once completed, the ruleset should be modified to reflect the changes.

Affects:

Device
FORTIFW01

SR-104-004	**Test / Temporary Rules Present**		△
Risk Rating	Low	**Status**	Open

Description:
A large number of rules were configured with a name that indicated they were either temporary or used for testing purposes. Whilst these temporary/test rules present no direct threat to security, they should be reviewed as a matter of 'good housekeeping' to establish whether they are required. Any which are required should be made permanent.

It is understood that a significant proportion of these rules are present to provide connectivity during the migration, of servers and their associated services from the legacy network. Particular attention should be paid to the removal of these rules following completion of this work, as several rules provide access to privileged hosts and services.

Full details of rules which appeared to be temporary or test related are detailed in the Supplemental Data - Test / Temporary Rules on page 29.

Recommendation:
The rules should be reviewed and removed if no longer required.

Affects:

Device
FORTIFW01

SR-104-005	Rules Allow Any ICMP Message Type		⚠
Risk Rating	Low	**Status**	Open

Description:
Rules were configured that allowed any ICMP message type between network segments. ICMP can be used to identify connected devices, and may be abused to exfiltrate data, where access controls ordinarily would restrict such action.

ICMP can be useful for network administrators who wish to determine if a network device is reachable or responding, but it can also be abused by an attacker to enumerate potential targets and learn more about them.

ICMP can also be used to tunnel traffic out of a network using a tool such as ICMPSh. Using this tool it may be possible for an attacker to exfiltrate data to an external host.

Rules which permitted all ICMP types are detailed below:

Root VDOM

Rule	Action	Source	Destination	Service
17	Allow	ZONE1_ADMINS_GROUP	TSZ_RDS_MGT_10.106.214.0/27 USZ_RDS_MGT_10.106.74.0/27 PSZ_RDS_MGT_10.106.183.0/26	HTTPS RDP ALL_ICMP
36	Allow	SolarWinds_10.193.145.80	UK_SITE1_FLBD01 UK_SITE1_FLBD02 UK_SITE1_FLBD_VIP	ALL_ICMP

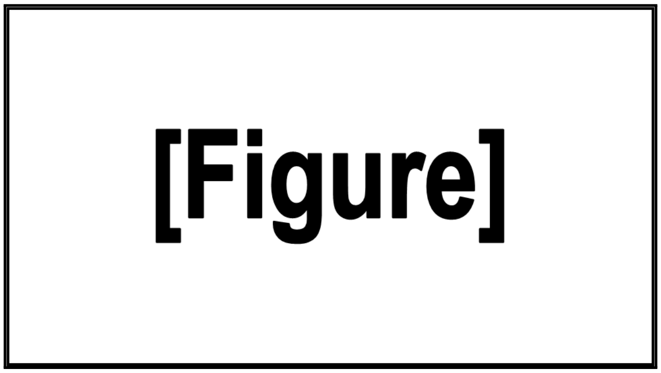

Figure 2: ZONE1-MGMT to SECUREZONE-MGMT-TOOL

Rule	Action	Source	Destination	Service
129	Allow	SolarWinds_10.193.145.80	MGMT_SZ_NET_ANY_10.106.193.64/26	SNMP ALL_ICMP

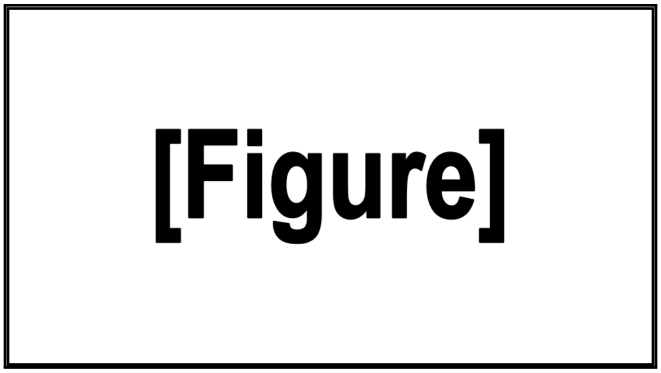

Figure 3: ZONE1-MGMT to SECUREZONE-MGM

Rule	Action	Source	Destination	Service
35	Allow	UK_SITE1_FLBD_VIP UK_SITE1_FLBD01 UK_SITE1_FLBD02	SolarWinds_10.193.145.80	ALL_ICMP

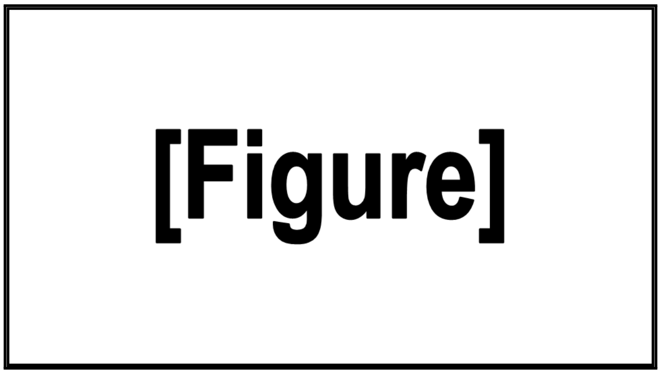

Figure 4: SECUREZONE-MGMT-TOOLS to ZONE1-MGM

Test VDOM

Rule	Action	Source	Destination	Service
54	Allow	ZONE1154_ANY_10.116.194.0/24 ZONE1155_ANY_10.116.174.0/24 ADMIN1_10.145.37.205	TSZ_CSV_BIZ_10.32.242.192/26	RDP ALL_ICMP

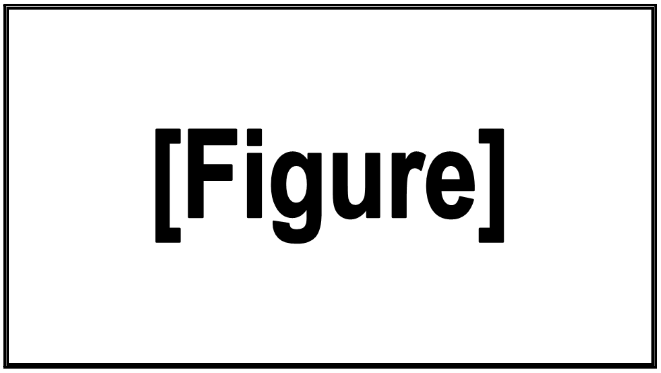

Figure 5: ZONE1-TEST to SECUREZONE-TEST-IN

Recommendation:

Rules should be configured to only allow ICMP messages between specific hosts or subnets, and in those instances specific message types should be specified.[2,3]

Affects:

Device
FORTIFW01

[2] **Common Exploits –ICMP Shell Fun** https://www.commonexploits.com/?p=896

[3] **ICMP Tunnelling** https://hackaday.com/2009/08/21/tunneling-ip-traffic-over-icmp/

SR-104-006	Proxy Address Resolution Protocol (ARP) was Enabled		△
Risk Rating	Low	Status	Open

Description:

The Proxy ARP feature, used to support ARP translation of IP addresses into MAC addresses across network segments and VLANs, was found to be supported. Permitting ARP packets to travel beyond the originating systems network segment may undermine network segmentation.

Proxy ARP is a legacy setting designed for hosts that do not have a default gateway configured. There is usually no good reason to have proxy ARP enabled in modern networks as it can allow attacks such as ARP spoofing.

Recommendation:

Proxy ARP functionality should be disabled, unless there is a significant business need. This should be done for each interface using the following command:

```
set arpforward disable
```

Affects:

Device
FORTIFW01

SR-104-007	ICMP Redirect Messages Were Enabled		△
Risk Rating	Low	**Status**	Open

Description:

Interfaces were configured to accept ICMP redirects. An attacker in a position to generate arbitrary ICMP packets may be able to manipulate the routing table to launch a man-in-the-middle attack.

ICMP redirect messages could be sent to the router in order to indicate a specific route that the sending host would like the network traffic to take. On a router that accepts ICMP redirect message the network traffic will be forwarded using the specified route. Furthermore, some routers will cache the new routing information for use with future network packets.

Recommendation:

ICMP redirect message sending can be disabled on network interfaces with the following command:

```
set icmp-redirect disable
```

Affects:

Device
FORTIFW01

SR-104-008	Network Time Source Not Authenticated		△
Risk Rating	Low	**Status**	Open

Description:

Although the firewall was configured to synchronise with a network time source, it did not utilise authentication. If an attacker was able to modify a device's time with an inaccurate time update, then it would be more difficult during an examination to correlate the system logs.

NTP (described in RFC 5905) is a complex time synchronisation protocol, with a number of different features and options such as time update authentication. Without authentication configured, an attacker could attempt to update the time by sending malicious time updates. An attacker could do this using open source code or by sending customised network packets, spoofing the source address.

Furthermore, any systems that depend on accurate time, such as some authentication systems, could be disrupted and potentially cause a denial of service.

Recommendation:

All networked devices should be synchronised by updating their clocks from an authenticated network time source, to preserve consistency between logs on different devices. FortiGate devices can be configured with the following commands:

```
config system ntp
    set ntpsync {enable | disable}
    set source-ip <ipv4_addr>
    set syncinterval <interval_int>
    set type {fortiguard | custom}
    set server-mode {enable | disable}
    set interface <interface_list>
    config ntpserver
        edit <serverid_int>
        set authentication {enable | disable}
        set key <password_str>
        set key-id <int>
        set ntpv3 {enable | disable}
        set server {<ipv4_addr> | <hostname_str> | <ipv4_addr>/<hostname_str>}
    end
end
```

Affects:

Device
FORTIFW01

SR-104-009	**Unrestricted Administrative Interfaces**		△
Risk Rating	Low	**Status**	Open

Description:

Access controls were not configured in order to restrict access to the firewalls management interfaces. As a result, an attacker would not be prevented from attempting to gain access to the device, or from exploiting any software vulnerabilities which were present.

Without any management host restrictions in place, an attacker or malicious user would be able to connect to the administrative services. If the service requires authentication and the attacker does not have any authentication credentials, they could attempt to gain access using a brute-force attack.

Furthermore, if a software vulnerability were present in the service then allowing anyone to connect to the service could enable an attacker to exploit the vulnerability.

Recommendation:

Access should be restricted to known management hosts. The following commands can be utilised to configure the firewall via the CLI:

```
config system admin
   edit admin
          set trusthost1 <ipv4_addr> <mask>
   end
end
```

Affects:

Device
FORTIFW01

SR-104-010	No Pre-Logon Banner Message		△
Risk Rating	Low	Status	Open

Description:

A login banner warning the user about any unauthorised access or referring to the Computer Misuse Act was not in use. It is recommended that a pre-logon banner is used to inform users of their rights prior to accessing a device.

Furthermore if legal proceedings were executed against an attacker it would be easier to prove intent on behalf of the attacker, if they were first warned against unauthorised access.

Recommendation:

A disclaimer should be configured, thereby ensuring users are aware of their legal and procedural responsibilities. General guidelines suggest that warning messages include at least the name of the organisation that owns the system, the fact that the system is subject to monitoring and that the use of the system implies consent to such monitoring.

The following command will enable the pre-login banner:

```
config system global
  set pre-login-banner enable
end
```

With the banner being configured as follows:

```
config system replacemsg admin "pre_admin-disclaimer-text"
    <warning>
end
```

Affects:

Device
FORTIFW01

SR-104-011	Local Based Authentication		⚠
Risk Rating	Low	**Status**	Open

Description:

The firewall was not configured to utilise a remote AAA solution such as Radius or TACACS+ for authentication, instead preferring the use of local users. Maintaining access and a secure password for a Group of administrators across a large number multiple network devices is not practical, administrators tend to compensate by using easy to remember passwords, or password reuse.

Recommendation:

Although it is recognised that the device is generally managed via FortiManager, it is consider best practice to utilise an authentication service for local access.

Configure the device to utilise RADIUS or TACACS+. The following commands can be used to add a TACACS+ server:

```
config system admin tacacs
  edit <name>
  set authen-type <auth_prot_type>
  set authorization {enable | disable}
  set key <password_string>
  set port <integer>
  set secondary-key <password_string>
  set secondary-server <string>
  set server <string>
  set tertiary-key <password_string>
  set tertiary-server <string>
end
```

Affects:

Device
FORTIFW01

SR-104-012	Duplicate / Overlapping Rules		
Risk Rating	Low	**Status**	Open

Description:

Rules that duplicated or overlapped one another were identified. Although not a direct threat to security, these rules could lead to confusion when administering the firewall. The clarity of a ruleset is important as confusion could lead to a configuration where access to services is overly permissive.

The following rules were identified:

VDOM UAT

Rule	Action	Source	Destination	Service
8	Allow	UATUK_SITE1_FDCS01_10.83.193.80 UATUK_SITE1_FDCS02_10.83.193.81	USZ_CSV_EXCH_10.83.193.128/26	AD_PORT_TCP/UDP
9	Allow	UATUK_SITE1_FDCS01_10.83.193.80 UATUK_SITE1_FDCS02_10.83.193.81	USZ_CSV_EXCH_10.83.193.128/26	AD_PORT_TCP/UDP

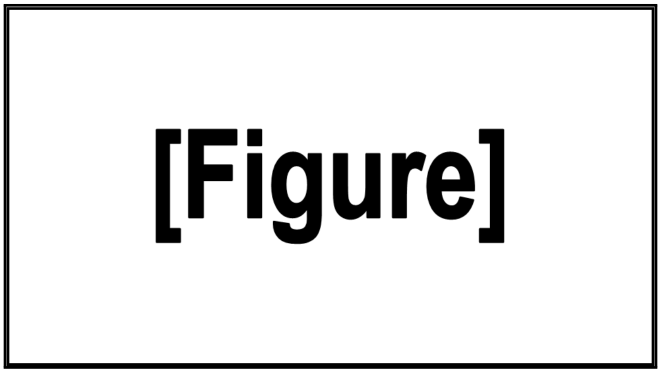

Figure 6: SECUREZONE-UAT-INF to SECUREZONE-UAT-IN

Rule	Action	Source	Destination	Service
41	Allow	USZ_RDS_MGT_10.106.74.0/27	UATUK_SITE1_FDCS01_10.83.193.80 UATUK_SITE1_FDCS02_10.83.193.81	AD_PORT_TCP/UDP
21	Allow	USZ_RDS_MGT_10.106.74.0/27	UATUK_SITE1_FDCS01_10.83.193.80 UATUK_SITE1_FDCS02_10.83.193.81	AD_PORT_TCP/UDP

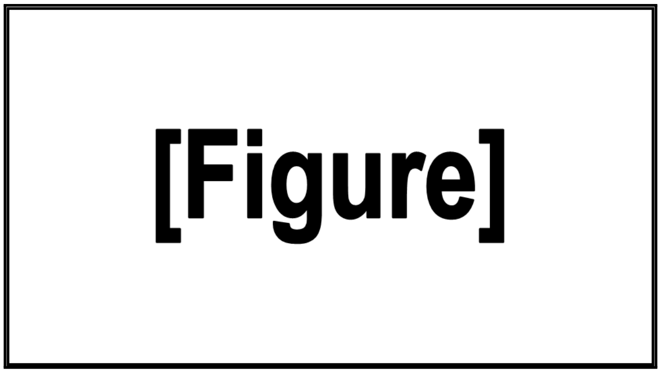

Figure 7: UAT-MGT to SECUREZONE-UAT-IN

Rule	Action	Source	Destination	Service
42	Allow	UATUK_SITE1_FDCS01_10.83.193.80 UATUK_SITE1_FDCS02_10.83.193.81	USZ_RDS_MGT_10.106.74.0/27	AD_PORT_TCP/UDP
22	Allow	UATUK_SITE1_FDCS01_10.83.193.80 UATUK_SITE1_FDCS02_10.83.193.81	USZ_RDS_MGT_10.106.74.0/27	AD_PORT_TCP/UDP

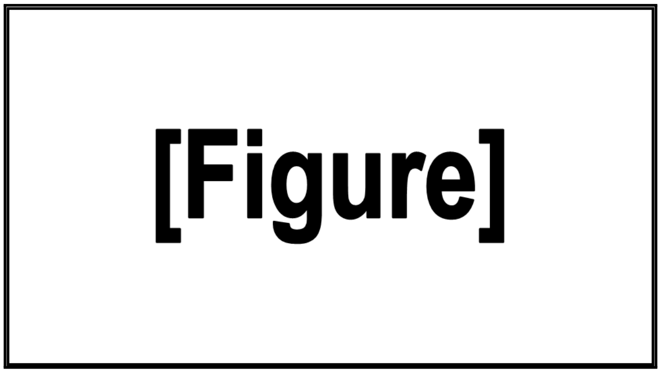

Figure 8: SECUREZONE-UAT-INF to UAT-MG

In addition, a number of rules within the Root VDOM were seen to utilise two service Groups which were nearly identical in their composure: AD_CLIENT_PORT_TCP/UDP & AD_PORT_TCP/UDP. The rules noted to be utilising these Groups were numbers 40, 89, 111, 112, 41, 33, 35, 46, 48, 76.

Recommendation:
Where possible, all rules should not duplicate or overlap others.

Affects:

Device
FORTIFW01

SR-104-013	**Disabled Rules Present**		ℹ
Risk Rating	Informational	**Status**	Open

Description:

A number of inactive rules were identified. Although not a direct threat to security, disabled rules can make network administration more difficult.

The ability to disable rules is useful for administrators who simply want to disable access to a service temporarily, for diagnostic purposes or to disable a rule which is planned to be re-activated again in the immediate future.

Despite this, disabled rules should not remain indefinitely and can make the policy configuration unclear to network administrators. This could lead to rules being configured that duplicate disabled rules and could potentially lead to mistakes with the policy configuration.

Rules which were identified as being inactive are detailed below:

Root VDOM

Rule	Action	Source	Destination	Service
190	Allow	UK_CTR_RDS01_10.193.145.230	PSZ_RDS_MGT_10.106.183.0/26 TSZ_RDS_MGT_10.106.214.0/27 USZ_RDS_MGT_10.106.74.0/27	DCE-RPC TCP/UDP_RPC_49152-50151

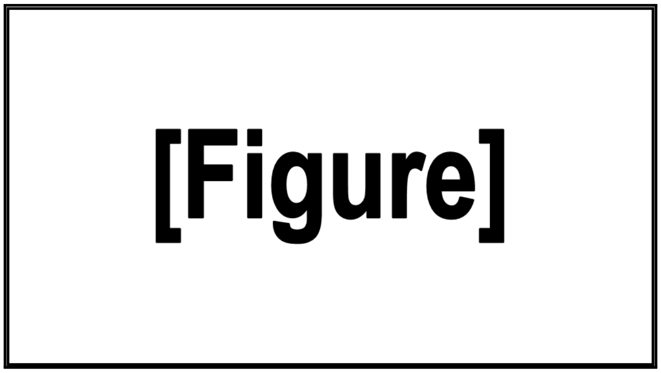

Figure 9: ZONE1-MGMT to SECUREZONE-MGMT-TOOL

Rule	Action	Source	Destination	Service
189	Allow	PSZ_RDS_MGT_10.106.183.0/26 TSZ_RDS_MGT_10.106.214.0/27 USZ_RDS_MGT_10.106.74.0/27	UK_CTR_RDS01_10.193.145.230	DCE-RPC TCP/UDP_RPC_49152-50151 TCP_5985_WinRM

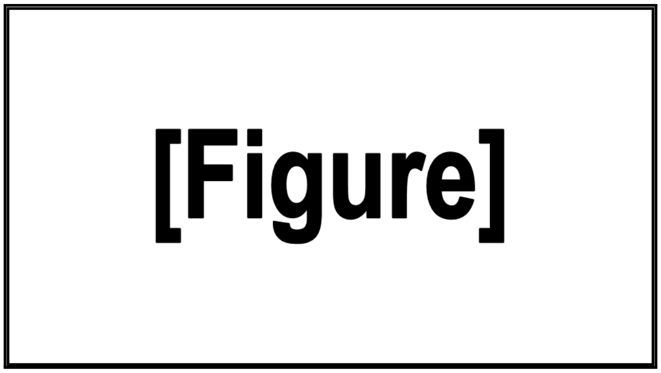

Figure 10: SECUREZONE-MGMT-TOOLS to ZONE1-MGM

Production VDOM

Rule	Action	Source	Destination	Service
84	Allow	PSZ_RDS_10.107.143.0/26	UK_SITE1_VL1_LINUXSVR_10.145.105.0/24 UK_SITE1_VL1_OTHSVR_10.145.200.0/24	HTTPS SMB SSH TCP_8080 TCP_RMI_50500

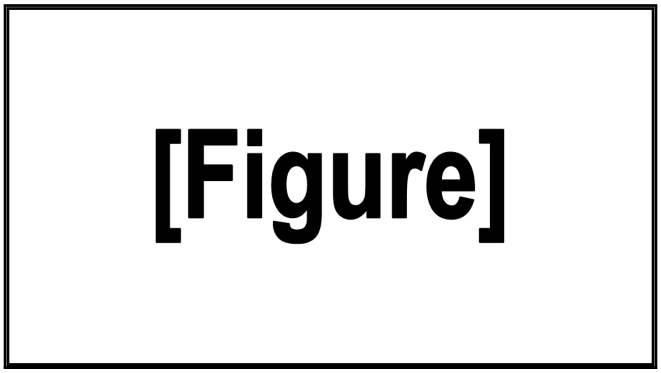

Figure 11: SECUREZONE-LIVE-INF to ZONE1-LIV

Recommendation:

Delete all disabled rules that are no longer required as a matter of 'good housekeeping'.

Affects:

Device
FORTIFW01

SR-104-014	Rules without Comment Text or Annotation		ℹ
Risk Rating	Informational	Status	Open

Description:

The majority of rules did not have a comment or annotation associated with them. Although not a threat to security, without comment text, the purpose of rules can be unclear making the administration of policies more difficult. This can lead to a situation where rules that are no longer required remain configured, giving an attacker additional access.

It is common for rules to initially be configured to allow access to a limited number of services and hosts and gradually grow over time as the business evolves and access to additional services or hosts are required. When access to a service is no longer required that related rule should be modified or removed. Without adequate tracking or change control, it may not be clear as to which rule applies to which service so the rule is not modified. In order to aid the clarity of rules, comment text can be included. This comment text is helpful in indicating why the rule exists.

Recommendation:

All rules should include a comment indicating its purpose.

Affects:

Device
FORTIFW01

5 Supplemental Data - Widely Scoped ACLs

Root VDOM

ZONE1-MGMT to SECUREZONE-MGMT-TOOLS

Rule	Action	Source	Destination	Service
174	Allow	GRP_RXK_NETS GRP_ACME_WIRELESS_NETS UK_SITE1_10.116.193.0/16	TSZ_RDS_MGT_10.106.214.0/27 USZ_RDS_MGT_10.106.74.0/27	HTTPS

ZONE1-MGMT to SECUREZONE-MGMT

Rule	Action	Source	Destination	Service
82	Allow	Cisco_ACS_10.145.193.91	MGMT_SZ_NET_ANY_10.106.193.64/26	ALL

SECUREZONE-MGMT to ZONE1-MGMT

Rule	Action	Source	Destination	Service
81	Allow	MGMT_SZ_NET_ANY_10.106.193.64/26	Cisco_ACS_10.145.193.91	ALL

6 Supplemental Data - Test / Temporary Rules

Root VDOM

ZONE1-MGMT to SECUREZONE-MGMT

Rule	Action	Source	Destination	Service
98	Allow	TEMP_AD_DNS_10.193.145.35 TEMP_AD_DNS_10.193.145.37	MGT_SZ_TOOLS_10.106.242.0/26	AD_PORT_TCP/UDP

ZONE1-MGMT to SECUREZONE-MGMT

Rule	Action	Source	Destination	Service
96	Allow	UK_CTR_DCS03_10.193.145.31 TEMP_AD_DNS_10.193.145.35	MGMT_SZ_NET_ANY_10.106.193.64/26	DNS
177	Allow	UK_CTR_DCS03_10.193.145.31 UK_SITE1_FDCS03_10.145.7.150 TEMP_LEGACY_DNS_10.145.7.4 TEMP_LEGACY_DNS_10.145.7.5 TEMP_LEGACY_DNS_10.145.7.6 TEMP_AD_DNS_10.193.145.35 TEMP_AD_DNS_10.193.145.37	PSZ_W2003_APP_MGT_10.106.129.96/27 PSZ_W2003_SRC_MGT_10.106.129.64/27	AD_PORT_TCP/UDP

SECUREZONE-MGMT to ZONE1-MGMT

Rule	Action	Source	Destination	Service
10	Allow	UK_SITE1_FSZDAMMGMTLB01	TEMP_LEGACY_DNS_10.145.7.4 TEMP_LEGACY_DNS_10.145.7.6 ACME_NTP_SERVERS UK_SITE1_FTSZDC01_ANY_10.32.242.80 TSTUK_SITE1_FDCS02_ANY_10.32.242.81	DNS NTP
95	Allow	MGMT_SZ_NET_ANY_10.106.193.64/26	UK_CTR_DCS03_10.193.145.31 TEMP_AD_DNS_10.193.145.35	DNS
76	Allow	DAM SZ Servers Test	orange-box.acme.com_10.145.105.130	HTTPS
77	Allow	CSV Biztalk Server Test	UK_CTR_APP04_AV_10.193.145.10	KAS_AV_CLIENT_TCP/UDP
93	Allow	USZ_APT_ALM_MGT_10.106.81.0/26	KMS Server TEMP	KMS_TCP_1688
175	Allow	PSZ_W2003_APP_MGT_10.106.129.96/27 PSZ_W2003_SRC_MGT_10.106.129.64/27	KMS Server TEMP	KMS_TCP_1688

Rule	Action	Source	Destination	Service
176	Allow	PSZ_W2003_APP_MGT_10.106.129.96/27 PSZ_W2003_SRC_MGT_10.106.129.64/27	UK_CTR_DCS03_10.193.145.31 UK_SITE1_FDCS03_10.145.7.150 TEMP_LEGACY_DNS_10.145.7.4 TEMP_LEGACY_DNS_10.145.7.5 TEMP_LEGACY_DNS_10.145.7.6 TEMP_AD_DNS_10.193.145.35 TEMP_AD_DNS_10.193.145.37	AD_PORT_TCP/UDP

7 Document Control

Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Client Company Ltd (ClientName).

NCC Group gives permission to copy this report for the purposes of disseminating information within your organisation or any regulatory agency.

7.1 Document Data

Data Classification	Client Confidential
Client Name	ClientName
Project Reference	99999
Proposal Reference	P99999-Sample
Document Title	FortiGate Firewall Review Sample Report
Author	NCC Consultant

7.2 Document History

Issue No.	Issue Date	Issued by	Change Description
0.1	2018-01-15	NCC Consultant	Draft for NCC Group internal review only
0.2	2018-01-16	A Reviewer	Revised QA
1.0	2018-01-16	NCC Consultant	Released to client
2.0	2018-02-14	NCC Consultant	Cover page address updated
3.0	2021-05-18	NCC Consultant	Minor content and format changes

7.3 Document Distribution List

Name	Role
A. Sponsor	Project Sponsor, ClientName
NCC Consultant	Senior Security Consultant, NCC Group
A. Manager	Account Manager, NCC Group

8 Assessment Team

The following members of staff were assigned to this assessment:

Name	Job Title	Comments
NCC Consultant	Senior Security Consultant, NCC Group	CREST Registered Tester (CRT)